AFF and FAS System Documentation

ONTAP Systems

NetApp
April 15, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems/index.html on April 15, 2022.
Always check docs.netapp.com for the latest.

Table of Contents

AFF and FAS System Documentation . . . 1
Get started . . . 2
What's new for FAS and AFF systems . . . 2
Release notes . . . 2
AFF systems . . . 3
AFF C190 System Documentation . . . 3
AFF A200 System Documentation . . . 82
A220 System Documentation . . . 158
AFF A250 System Documentation . . . 281
AFF A300 System Documentation . . . 376
AFF A320 System Documentation . . . 488
AFF A400 System Documentation . . . 575
AFF A700 System Documentation . . . 691
AFF A700s System Documentation . . . 839
AFF A800 System Documentation . . . 931
AFF A900 systems . . . 1039
FAS systems . . . 1152
FAS500f System Documentation . . . 1152
FAS2600 System Documentation . . . 1247
FAS2700 System Documentation . . . 1332
FAS8200 System Documentation . . . 1455
FAS8300 and FAS8700 System Documentation . . . 1575
FAS9000 System Documentation . . . 1705
All SAN Array systems . . . 1853
Upgrade procedures . . . 1854
System-level diagnostics . . . 1855
Introduction to system-level diagnostics . . . 1855
Requirements for running system-level diagnostics . . . 1855
How to use online command-line help . . . 1857
Run system installation diagnostics . . . 1858
Run system panic diagnostics . . . 1861
Run slow system response diagnostics . . . 1864
Run hardware installation diagnostics . . . 1868
Run device failure diagnostics . . . 1871
Drive shelves . . . 1876
NS224 shelves . . . 1876
SAS shelves with IOM12 modules . . . 1925
Switches . . . 2054
Cabinet and rail kits . . . 2055
SuperRail kit installation instructions . . . 2055
Two-post support rail kit installation instructions - AFF A700 and FAS9000 . . . 2056
42U 1280 mm system cabinet . . . 2058
Other models . . . 2083

Platform models . . . 2083
Shelf models . . . 2083
Legal notices . . . 2084
Copyright . . . 2084
Trademarks . . . 2084
Patents . . . 2084
Privacy policy . . . 2084
Open source . . . 2084

AFF and FAS System Documentation

Get started

What's new for FAS and AFF systems

Learn about the new features for FAS and AFF systems.

New adapter support

Unresolved directive in whats-new.adoc - include::../_include/new-adapter.adoc[]

New switch support

Unresolved directive in whats-new.adoc - include::../_include/new-switch-support.adoc[]

New platform support

Unresolved directive in whats-new.adoc - include::../_include/new-platform-support.adoc[]

New shelf support

Unresolved directive in whats-new.adoc - include::../_include/new-shelf-support.adoc[]

New hardware updates

Unresolved directive in whats-new.adoc - include::../_include/new-hardware-updates.adoc[]

New hardware upgrade enhancements

Unresolved directive in whats-new.adoc - include::../_include/new-hardware-enhancements.adoc[]

Release notes

Release notes are available outside this site. You will be prompted to log in using your NetApp Support Site credentials.

Access the ONTAP 9 Release Notes

AFF systems

AFF C190 System Documentation

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 C190

This section gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use the AFF C190 Systems Installation and Setup Instructions if you are familiar with installing NetApp systems.

Videos - AFF C190

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

Video one of two: Hardware installation and cabling

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

Installation and Setup of an AFF C190

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

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

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

Detailed steps - AFF C190

This section gives detailed step-by-step instructions for installing a AFF C190 system.

Step 1: Prepare for installation

To install your AFF C190 system, you need to create an account and register the system. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

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

What you need

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
- A laptop or console with an RJ-45 connection and access to a Web browser

Steps

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

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

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

Type of cable…	Part number and length	Connector type	For…
10 GbE cable (order dependent)	X6566B-05-R6 (112-00297), 0.5m X6566B-2-R6 (112-00299), 2m		Cluster interconnect network
	X6566B-2-R6 (112-00299), 2m X6566B-3-R6 (112-00300), 3m X6566B-5-R6 (112-00301), 5m		Data

Type of cable…	Part number and length	Connector type	For…
Optical network cables (order dependent)	X6553-R6 (112-00188), 2m X6536-R6 (112-00090), 5m X6554-R6(112-00189), 15m		SFP + FC host network
Cat 6, RJ-45 (order dependent)	X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Ethernet host and management network
Micro-USB console cable	Not applicable		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	Not applicable		Powering up the system

6. Download and complete the Cluster Configuration Worksheet.

Step 2: Install the hardware

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

Steps

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

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

3. Attach cable management devices (as shown).

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

Step 3: Cable controllers to your network

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

Option 1: Cable a two-node switchless cluster, unified configuration

UTA2 ports and management ports on the controller modules are connected to switches. The cluster interconnect ports are cabled on both controller modules.

Before you begin

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

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

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

> If connecting to an optical switch, insert the SFP into the controller port before cabling to the port.

Steps

1. Use the illustration or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the cluster interconnect cable: • e0a to e0a • e0b to e0b
2	Use one of the following cable types to cable the e0c/0c and e0d/0d **or** e0e/0e and e0f/0f data ports to your host network:

Step	Perform on each controller
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

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

Option 2: Cable switched cluster, unified configuration

UTA2 ports and management ports on the controller modules are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

Before you begin

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

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

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

If connecting to an optical switch, insert the SFP into the controller port before cabling to the port.

Steps

1. Use the illustration or the step-by-step instructions to complete the cabling between the controllers and the switches:

Step	Perform on each controller module
1	Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:
2	Use one of the following cable types to cable the e0c/0c and e0d/0d **or** e0e/0e and e0f/0f data ports to your host network:

Step	Perform on each controller module
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

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

Option 3: Cable a two node switchless cluster, Ethernet configuration

RJ45 ports and management ports on the controller modules are connected to switches. The cluster interconnect ports are cabled on both controller modules.

Before you begin

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

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

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

Steps

1. Use the illustration or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the cluster interconnect cable : • e0a to e0a • e0b to e0b
2	Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:

Step	Perform on each controller
3	Cable the e0M ports to the management network switches with the RJ45 cables .
!	DO NOT plug in the power cords at this point.

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

Option 4: Cable a switched cluster, Ethernet configuration

RJ45 ports and management ports on the controller modules are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

Before you begin

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

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

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

Steps

1. Use the illustration or the step-by-step instructions to complete the cabling between the controllers and the switches:

Step	Perform on each controller module
1	Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:
2	Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:

Step	Perform on each controller module
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

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

Step 4: Complete system setup and configuration

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

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

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

Steps

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

Initial booting may take up to eight minutes..

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

   See your laptop's online help for more information.

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

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

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

   System Manager opens.

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

> The default port configuration for Unified configuration systems is CNA mode; if connecting to an FC host network, you have to modify the ports for FC mode.

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

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

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

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

b. Connect the console cable to the laptop or console, and connect the console port on the controller using the console cable that came with your system.

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

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

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

Initial booting may take up to eight minutes..

4. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.

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

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

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

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

The default port configuration for Unified configuration systems is CNA mode; if connecting to an FC host network, you have to modify the ports for FC mode.

Maintain

Boot media

Overview of boot media replacement - AFF C190

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

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

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

- The *healthy* controller is the HA partner of the impaired controller.

Check onboard encryption keys - AFF C190

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

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

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

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Check NVE or NSE on systems running ONTAP 9.6 and later

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

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

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

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

Verify NVE configuration

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

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

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

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

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

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

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

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

Verify NSE configuration

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

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

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

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

e. You can safely shut down the controller.

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

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

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

   c. You can safely shut down the controller.

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

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

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

      mysupport.netapp.com

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

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

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

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

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

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

   h. You can safely shut down the controller.

Shut down the controller - AFF C190

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

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

Replace the boot media - AFF C190

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

Step 1: Remove the controller

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

Steps

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

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

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

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

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

Step 2: Replace the boot media

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

1. Locate the boot media using the following illustration or the FRU map on the controller module:
2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

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

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

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

Step 3: Transfer the boot image to the boot media

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

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

Steps

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

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

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

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

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

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

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

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

6. Boot the recovery image:

   `boot_recovery` *`ontap_image_name`*`.tgz`

   > If the `image.tgz` file is named something other than image.tgz, such as `boot_recovery 9_4.tgz`, you need to include the different file name in the `boot_recovery` command.

   The system boots to the boot menu and prompts you for the boot image name.

7. Enter the boot image name that is on the USB flash drive:

   ***`image_name`*`.tgz`**

   After `image_name.tgz` is installed, the system prompts you to restore the backup configuration (the `var` file system) from the healthy controller.

8. Restore the `var` file system:

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

9. Verify that the environmental variables are set as expected.
   a. Take the controller to the LOADER prompt.

      From the ONTAP prompt, you can issue the command `system node halt -skip-lif -migration-before-shutdown true -ignore-quorum-warnings true -inhibit -takeover true`.

   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.
   e. Reboot the controller.
10. The next step depends on your system configuration:

If your system is in…	Then…
A stand-alone configuration	You can begin using your system after the controller reboots.
An HA pair	After the impaired controller is displaying the `Waiting for Giveback…` message, perform a giveback from the healthy controller: a. Perform a giveback from the healthy controller: **`storage failover giveback -ofnode`** ***`partner_node_name`*** This initiates the process of returning ownership of the impaired controller's aggregates and volumes from the healthy controller back to the impaired controller. If the giveback is vetoed, you can consider overriding the vetoes. ONTAP 9 High-Availability Configuration Guide b. Monitor the progress of the giveback operation by using the `` `storage failover show`-giveback` `` command. c. After the giveback operation is complete, confirm that the HA pair is healthy and that takeover is possible by using the `storage failover show` command. d. Restore automatic giveback if you disabled it by using the `storage failover modify` command.

Boot the recovery image - AFF C190

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

Steps

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

   ```
   boot_recovery
   ```

   The image is downloaded from the USB flash drive.

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

If your system has…	Then…

A network connection	a. Press **y** when prompted to restore the backup configuration.
	b. Set the healthy controller to advanced privilege level:
	`set -privilege advanced`
	c. Run the restore backup command:
	`system node restore-backup -node local -target -address impaired_node_IP_address`
	d. Return the controller to admin level:
	`set -privilege admin`
	e. Press **y** when prompted to use the restored configuration.
	f. Press **y** when prompted to reboot the controller.

No network connection	a. Press **n** when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press **y**.

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

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

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

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

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

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

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

Restore OKM, NSE, and NVE as needed - AFF C190

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

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

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

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

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

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

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

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

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


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

   The system boots to Waiting for giveback… prompt.

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

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

      Terminating CIFS can cause loss of data.

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

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

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

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

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

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

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

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

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

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

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

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

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

     Terminating CIFS can cause loss of data.

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

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

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

  > If the command fails, contact Customer Support.

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

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

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

Return the failed part to NetApp - AFF C190

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF C190

To replace the chassis, you must move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

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

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF C190

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

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or

a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

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

Steps

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

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

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

   The confirmation message looks like the following:

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

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

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

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

   Answer `y` when prompted.

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

Step 1: Move the power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.
4. Use the cam handle to slide the power supply out of the system.

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

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

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

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

7. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

Step 2: 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. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

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

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

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

Step 3: Move drives to the new chassis

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

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

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

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

      Drives are fragile. Handle them as little as possible to prevent damage to them.

3. Align the drive from the old chassis with the same bay opening in the new chassis.

4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.

5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.

6. Repeat the process for the remaining drives in the system.

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

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

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

Step 5: Install the controller module

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

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

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

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

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module
   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. Repeat the preceding steps for the second controller module in the new chassis.

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

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

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

Restore and verify the configuration - AFF C190

You must verify the HA state of the chassis and run System-Level diagnostics.

Step 1: Verify 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`

   b. Confirm that the setting has changed:

      `ha-config show`

3. If you have not already done so, recable the rest of your system.
4. The next step depends on your system configuration.

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

Step 2: Run system-level diagnostics

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

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

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

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

      ```
      halt
      ```

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

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

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

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

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

   ```
   boot_diags
   ```

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

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt:

   ```
   sldiag device modify -dev interconnect -sel enable
   ```

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

5. Run the interconnect diagnostics test from the Maintenance mode prompt:

   `sldiag device run -dev interconnect`

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

6. Verify that no hardware problems resulted from the replacement of the chassis:

   `sldiag device status -dev interconnect -long -state failed`

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

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

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

If your system is running ONTAP…	Then…

With two nodes in the cluster	Issue these commands:
	
	`node::> cluster ha modify -configured true`
	
	`node::> storage failover modify -node node0 -enabled true`

With more than two nodes in the cluster	Issue this command: `node::> storage failover modify -node node0 -enabled true`
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - AFF C190

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

- All drive shelves must be working properly.

- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system’s configuration.
- You should perform the drive reassignment as directed in the procedure.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller’s console output to a text file.

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

Shut down the controller - AFF C190

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

Replace the controller module hardware - AFF C190

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

Step 1: Remove controller module

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

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

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

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

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

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

Step 2: Move the boot media

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

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

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

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

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

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

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

Step 3: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

- If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
- If the LED is on and power is on, unwritten data is stored on NVMEM.

  This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

   The number and placement of system DIMMs depends on the model of your system.

   The following illustration shows the location of system DIMMs:

4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

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

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

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

Make sure that the plug locks down onto the controller module.

Step 5: Install the controller module

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

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

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

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

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

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

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

4. Complete the reinstallation of the controller module. The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   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. Interrupt the boot process **only** after determining the correct timing:

      You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete.

      Only press `Ctrl-C` when you see the message `Press Ctrl-C for Boot Menu`.

      > If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort.

If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.

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

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

e. Select the option to boot to Maintenance mode from the displayed menu.

Restore and verify the system configuration - AFF C190

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

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

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

About this task

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

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

Steps

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

   The date and time are given in GMT.

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

   The date and time are given in GMT.

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

   The date and time are given in GMT.

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

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

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

   The HA state should be the same for all components.

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

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

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

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

Step 3: Run system-level diagnostics

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

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

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

   `halt`

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

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

   `boot_diags`

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

3. Display and note the available devices on the controller module:

   `sldiag device show -dev mb`

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

- `bootmedia` is the system booting device.
- `cna` is a Converged Network Adapter or interface not connected to a network or storage device.
- `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
- `env` is motherboard environmentals.
- `mem` is system memory.
- `nic` is a network interface card.
- `nvram` is nonvolatile RAM.
- `nvmem` is a hybrid of NVRAM and system memory.
- `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: **`sldiag device clearstatus`** b. Display the available tests for the selected devices: **`sldiag device show -dev dev_name`** *`dev_name`* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: **`sldiag device modify -dev dev_name -selection only`** -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: **`sldiag device run -dev dev_name`** After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: **`sldiag device status -dev dev_name -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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: **`sldiag device show -dev dev_name`** c. Examine the output and, if applicable, select only the tests that you want to run: **`sldiag device modify -dev dev_name -selection only`** -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: **`sldiag device show`** e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: **`sldiag device run`** Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: **`sldiag device status -long -state failed`** System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

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

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: **`sldiag device clearstatus`** b. Verify that the log was cleared: **`sldiag device status`** The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: **`halt`** The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: **`halt`** b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - AFF C190

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

Step 1: Recable the system

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

Steps

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

Step 2: Verifying the system ID change on an HA system

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

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

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt:

   `halt`

2. From the LOADER prompt on the *replacement* controller, boot the controller, entering **`y`** if you are prompted to override the system ID due to a system ID mismatch.
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned:

   `` `storage failover show` ``

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

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

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level:

`set -privilege advanced`

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

b. Save any coredumps:

`system node run -node local-node-name partner savecore`

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

You can enter the following command to monitor the progress of the savecore command:

`system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level:

`set -privilege admin`

5. Give back the controller:

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

`storage failover giveback -ofnode replacement_node_name`

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

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

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

Find the High-Availability Configuration content for your version of ONTAP 9

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

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

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

The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

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

7. Verify that the expected volumes are present for each controller:

   `vol show -node node-name`

8. If you disabled automatic takeover on reboot, enable it from the healthy controller:

   `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF C190

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

Step 1: Installing licenses for the *replacement* controller in ONTAP

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

About this task

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

Before you begin

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

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

Steps

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

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

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

Step 2: Restoring Storage and Volume Encryption functionality

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

Step

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

Step 3: Verifying LIFs and registering the serial number

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

Steps

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

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

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-

638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF C190

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

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

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

Step 1: Shut down the impaired controller

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

About this task

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

Step 2: Remove controller module

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

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

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

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

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

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

Step 3: Replace the DIMMs

To replace the DIMMs, you need to locate them inside the controller module, and then follow the specific sequence of steps.

If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

1. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

2. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
3. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:
   a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.

b. Confirm that the NVMEM LED is no longer lit.

c. Reconnect the battery connector.

4. Return to Step 3: Replace the DIMMs of this procedure to recheck the NVMEM LED.
5. Locate the DIMMs on your controller module.

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

6. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
7. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

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

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

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

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

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

10. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
11. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

12. Close the controller module cover.

Step 4: Reinstall the controller module

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

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

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

3. Recable the system, as needed.

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

4. Complete the reinstallation of the controller module. The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.

      > If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.

   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:

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

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

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

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

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

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

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

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* **Note:** If you disabled automatic giveback, re-enable it with the storage failover modify command.
A stand-alone configuration	Proceed to the next step. No action is required. + You have completed system-level diagnostics.

Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF C190

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

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

Before you begin

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

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

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

- Determine whether SED authentication is enabled.

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

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

About this task

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

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

Procedure

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

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

Option 1: Replace SSD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.

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

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

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

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

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

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

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

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

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

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

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

      You can enter the command on either controller module.

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

      You can enter the command on either controller module.

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

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

      You must reenable automatic drive assignment on both controller modules.

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

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

Option 2: Replace HDD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.

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

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

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

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

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

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

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

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

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

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

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

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

       You can enter the command on either controller module.

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

       You can enter the command on either controller module.

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

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

       You must reenable automatic drive assignment on both controller modules.

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

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

Replace the NVMEM battery - AFF C190

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

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

Step 1: Shut down the impaired controller

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

About this task

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

Step 2: Remove controller module

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

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

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

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

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

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

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.
>
> - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
> - If the LED is on and power is on, unwritten data is stored on NVMEM.
>
> This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Remove the battery from the controller module and set it aside.
5. Remove the replacement battery from its package.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
9. Plug the battery plug back into the controller module.

Step 4: Reinstall the controller module

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

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

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

3. Recable the system, as needed.

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

4. Complete the reinstallation of the controller module. The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   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. When you see the message `Press Ctrl-C for Boot Menu`, press **`Ctrl-C`** to interrupt the boot process.

      > If you miss the prompt and the controller module boots to ONTAP, enter **`halt`**, and then at the LOADER prompt enter **`boot_ontap`**, press **`Ctrl-C`** when prompted, and then boot to Maintenance mode.

   e. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

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

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

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

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

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

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

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

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

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

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

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

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF C190

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

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

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

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

- Power supplies are auto-ranging.

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

5. Use the cam handle to slide the power supply out of the system.

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

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

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

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

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

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

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

   The power supply LEDs are lit when the power supply comes online.

2. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

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

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

Step 1: Shut down the impaired controller

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

About this task

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

Step 2: Remove controller module

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

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

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

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

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

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

Step 3: Replace the RTC battery

To replace the RTC battery, you need to locate it inside the controller module, and then follow the specific sequence of steps.

1. Locate the RTC battery.

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

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

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

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

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

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

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

3. Recable the system, as needed.

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

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module. The controller module begins to boot as soon as it is fully seated in the chassis.
   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. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.

c. If necessary, modify the date with the `set date mm/dd/yyyy` command.

d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.

e. Confirm the date and time on the target controller.

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Complete the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

AFF A200 System Documentation

Install and setup

Cluster configuration worksheet - AFF A200

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

Start here: Choose your installation and setup experience

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

- Quick steps

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

- Video steps

  Video step-by-step instructions.

Installation and setup PDF poster - AFF A200

You can use the AFF A200 Installation and Setup Instructions poster to install and set up your new system. The PDF poster provides step-by-step instructions with live links to additional content.

Installation and setup video - AFF A200

The AFF A200 Setup Video shows end-to-end software configuration for systems running ONTAP 9.2.

Maintain

Boot media

Overview of boot media replacement - AFF A200

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.

What you'll need

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

Before you begin

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

Check onboard encryption keys - AFF A200

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

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

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

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

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <Ino-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <Ino-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <Ino-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

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

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

Steps

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

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

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

Verify NVE configuration

Steps

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

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

c. Shut down the impaired controller.

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

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

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

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

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

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

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

Verify NSE configuration

Steps

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

   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.

- If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

   c. Shut down the impaired controller.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Verify NVE configuration

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

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

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

`key-manager external restore`

If the command fails, contact NetApp Support.

mysupport.netapp.com

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

c. Shut down the impaired controller.

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

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

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

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

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

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

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

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

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

h. You can safely shut down the controller.

Verify NSE configuration

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

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

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

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

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

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

      mysupport.netapp.com

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

Shut down the impaired controller - AFF A200

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

Replace the boot media - AFF A200

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

Step 1: Remove the controller

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

Steps

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

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

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

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

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

Step 2: Replace the boot media

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:
3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

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

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

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

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image

installed on it. However, you must restore the var file system during this procedure.

What you'll need

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

Steps

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

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

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

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

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

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

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

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

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

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

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

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

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

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask`

`-gw=gateway-dns=dns_addr-domain=dns_domain`

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

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

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

Boot the recovery image - AFF A200

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

Steps

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

   The image is downloaded from the USB flash drive.

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

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.

If your system has…	Then…
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `saveenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

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

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.
10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

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

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

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

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

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

Steps

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

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

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

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

Example of backup data:

```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

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


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

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

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

      > Terminating CIFS can cause loss of data.

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

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

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.

b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

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

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

14. If you are running ONTAP 9.6 or later:

    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.

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

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

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

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

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

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

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

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

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

Steps

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

If the console displays…	Then…
The login prompt	Go to Step 7.

If the console displays…	Then…
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

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

     Terminating CIFS can cause loss of data.

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

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

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

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

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

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

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

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

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

Steps

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

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

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

     Terminating CIFS can cause loss of data.
   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

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

      If the command fails, contact Customer Support.

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

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

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

Return the failed part to NetApp - AFF A200

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A200

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

chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

What you'll need

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

About this task

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A200

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

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

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

Steps

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

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

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

   The confirmation message looks like the following:

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

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

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

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

   Answer `y` when prompted.

Move and replace hardware - AFF A200

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

Step 1: Move the power supply

Move the power supply from the old chassis to the replacement chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.
4. Use the cam handle to slide the power supply out of the system.

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

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

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

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

7. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

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

Step 2: Remove the controller module

Remove the controller module or modules from the old chassis.

Steps

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

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

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

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

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

Step 3: Move drives to the new chassis

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

Steps

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

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

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

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

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

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

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

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

Steps

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

Step 5: Install the controller

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

About this task

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

Steps

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

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

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Repeat the preceding steps for the second controller module in the new chassis.
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Reinstall the blanking panel and then go to the next step.

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

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

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

Restore and verify the configuration - AFF A200

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

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

Steps

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

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:

   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

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

      - `ha`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.

Step 2: Running system-level diagnostics

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

What you'll need

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

About this task

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

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:

   a. Select the Maintenance mode option from the displayed menu.

   b. After the controller boots to Maintenance mode, halt the controller: `halt`

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

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

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

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

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

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

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

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

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

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

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

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

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

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

If your system is running ONTAP…	**Then…**
With two controllers in the cluster	Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true`
With more than two controllers in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If your system is running ONTAP…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - AFF A200

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

What you'll need

- All drive shelves must be working properly.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the "impaired node").

About this task

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must replace 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* node so that the *replacement* node will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* node is the controller that is being replaced.
  - The *replacement* node is the new controller that is replacing the impaired controller.

- The *healthy* node 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 A200

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

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

Replace the controller module hardware - AFF A200

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

move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove controller module

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

Steps

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

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

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

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

6. Turn the controller module over and place it on a flat, stable surface.

7. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Move the boot media

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

Steps

1. Locate the boot media using the following illustration or the FRU map on the controller module:
2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

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

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

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

Step 3: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a

specific sequence of steps.

Steps

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.

5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

About this task

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

Steps

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

   The number and placement of system DIMMs depends on the model of your system.

   The following illustration shows the location of system DIMMs:

4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

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

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

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

   Make sure that the plug locks down onto the controller module.

Step 5: Install the controller

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

About this task

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

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

Steps

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

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

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

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

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

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

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

Restore and verify the system configuration - AFF A200

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

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

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

About this task

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

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

Steps

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

   The date and time are given in GMT.

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

   The date and time are given in GMT.

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

   The date and time are given in GMT.

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

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

Steps

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

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

   - ha
   - non-ha

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

Step 3: Run system-level diagnostics

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

About this task

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

Steps

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

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

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

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

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

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

   - `bootmedia` is the system booting device..
   - cna is a Converged Network Adapter or interface not connected to a network or storage device.
   - fcal is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - mem is system memory.
   - nic is a network interface card.
   - `nvram` is nonvolatile RAM.
   - `nvmem` is a hybrid of NVRAM and system memory.
   - `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`* *dev_name* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev` *`dev_name`* After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

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

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - AFF A200

Continue the replacement procedure by re-cabling the storage and confirming disk reassignment.

Step 1: Re-cable the system

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

Steps

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

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks. You must use the correct procedure for your configuration.

Option 1: Verify the system ID change on an HA system

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

About this task

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.`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

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

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

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

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

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

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

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

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

5. Give back the controller:

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

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

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

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

      Find the High-Availability Configuration content for your version of ONTAP 9

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

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

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

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

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

7. Verify that the expected volumes are present for each controller: `vol show -node node-name`

8. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Option 2: Manually reassign the system ID on a stand-alone system in ONTAP

In a stand-alone system, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems that are in a stand-alone configuration.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.
2. You must enter `Y` when prompted to override the system ID due to a system ID mismatch.
3. View the system IDs: `disk show -a`
4. You should make a note of the old system ID, which is displayed as part of the disk owner column.

   The following example shows the old system ID of 118073209:

   ```
   *> disk show -a
   Local System ID: 118065481

     DISK      OWNER                   POOL   SERIAL NUMBER  HOME
   --------    -------------           -----  -------------  -------------
   disk_name    system-1  (118073209)  Pool0  J8XJE9LC       system-1
   (118073209)
   disk_name    system-1  (118073209)  Pool0  J8Y478RC       system-1
   (118073209)
   .
   .
   .
   ```

5. Reassign disk ownership by using the system ID information obtained from the disk show command: `disk reassign -s old system ID disk reassign -s 118073209`
6. Verify that the disks were assigned correctly: `disk show -a`

   The disks belonging to the replacement node should show the new system ID. The following example now show the disks owned by system-1 the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

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

7. Boot the node: `boot_ontap`

Complete system restoration - AFF A200

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

Step 1: Install licenses for the replacement controller in ONTAP

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

About this task

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

Before you begin

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

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

Steps

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

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

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

Step 2: Restore Storage and Volume Encryption functionality

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

Step

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

Step 3: Verify LIFs and registering the serial number

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

Steps

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

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

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A200

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.

About this task

- All other components in the system must be functioning properly; if not, you must contact technical support.
- You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

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

About this task

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

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

Step 2: Remove controller module

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

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

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

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

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

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

Step 3: Replace the DIMMs

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

About this task

If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

3. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
4. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:
   a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug

socket, and then unplug the battery cable from the socket.

b. Confirm that the NVMEM LED is no longer lit.

c. Reconnect the battery connector.

5. Return to step 2 of this procedure to recheck the NVMEM LED.
6. Locate the DIMMs on your controller module.

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

7. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
8. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

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

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

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

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

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

11. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
12. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

13. Close the controller module cover.

Step 4: Reinstall the controller module

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

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

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

4. Recable the system, as needed.

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

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. ⓘ 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

What you'll need

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

About this task

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

Steps

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

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

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

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

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

appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

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

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

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

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

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

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

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

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF A200

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

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

Before you begin

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

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

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

- Determine whether SED authentication is enabled.

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

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

About this task

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

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

Procedure

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

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

Option 1: Replace SSD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.

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

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

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

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

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

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

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

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

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

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

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

      You can enter the command on either controller module.

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

      You can enter the command on either controller module.

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

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

      You must reenable automatic drive assignment on both controller modules.

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

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

Option 2: Replace HDD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.

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

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

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

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

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

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

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

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

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

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

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

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

       You can enter the command on either controller module.

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

       You can enter the command on either controller module.

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

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

       You must reenable automatic drive assignment on both controller modules.

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

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

Replace the NVMEM battery - AFF A200

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

About this task

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 different procedures, depending on the storage system hardware configuration.

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

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

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

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

Step 2: Remove controller module

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

Steps

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

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

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

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

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

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

Steps

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

3. Locate the NVMEM battery in the controller module.

4. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
5. Remove the battery from the controller module and set it aside.
6. Remove the replacement battery from its package.

7. Loop the battery cable around the cable channel on the side of the battery holder.
8. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
9. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
10. Plug the battery plug back into the controller module.

Step 4: Reinstall the controller module

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

Steps

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

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

4. Recable the system, as needed.

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

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

What you'll need

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

About this task

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

Steps

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

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

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

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

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

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

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

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

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

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

If your controller is in…	**Then…**
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A200

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.

What you'll need

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.

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

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

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

   If you have an AFF A200 system, a plastic flap within the now empty slot is released to cover the opening and maintain air flow and cooling.

5. Use the cam handle to slide the power supply out of the system.

   > When removing a power supply, always use two hands to support its weight.

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   > Do not use excessive force when sliding the power supply into the system. You can damage the connector.

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.

b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

10. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

    The power supply LEDs are lit when the power supply comes online.

11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A200

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.

About this task

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and set time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

Steps

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy 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

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

A220 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick guide - AFF A220 and FAS2700

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A220/FAS2700 Systems Installation and Setup Instructions

Videos - AFF A220 and FAS2700

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

NetApp video: AFF A220 and FAS2700 Systems: Installation and Setup Instructions

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - AFF A220 and FAS2700

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Step 1: Prepare for installation

To install your FAS2700 or AFF A220 system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
- A laptop or console with an RJ-45 connection and access to a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register your system.

      NetApp Product Registration

4. Download and install Config Advisor on your laptop.

   NetApp Downloads: Config Advisor

5. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
10 GbE cable (order dependent)	X6566B-05-R6 (112-00297), 0.5m X6566B-2-R6 (112-00299), 2m		Cluster interconnect network
10 GbE cable (order dependent)	Part number X6566B-2-R6 (112-00299), 2m or X6566B-3-R6 (112-00300), 3m X6566B-5-R6 (112-00301), 5m		Data
Optical network cables (order dependent)	X6553-R6 (112-00188), 2m X6536-R6 (112-00090), 5m X6554-R6(112-00189), 15m		FC host network
Cat 6, RJ-45 (order dependent)	Part numbers X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network and Ethernet data
Storage (order dependent)	Part number X66030A (112-00435), 0.5m X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		Storage
Micro-USB console cable	Not applicable		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	Not applicable		Powering up the system

6. Download and complete the *Cluster configuration worksheet*.

   Cluster Configuration Worksheet

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

You need to be aware of the safety concerns associated with the weight of the system.

3. Attach cable management devices (as shown).

4. Place the bezel on the front of the system.

Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster, unified network configuration

Management network, UTA2 data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the cluster interconnect cable: • e0a to e0a • e0b to e0b

Step	Perform on each controller
2	Use one of the following cable types to cable the UTA2 data ports to your host network: An FC host • 0c and 0d • **or** 0e and 0f A 10GbE • e0c and e0d • **or** e0e and e0f You can connect one port pair as CNA and one port pair as FC, or you can connect both port pairs as CNA or both port pairs as FC.
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Option 2: Cable a switched cluster, unified network configuration

Management network, UTA2 data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and the switches:

Step	Perform on each controller module
1	Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:
2	Use one of the following cable types to cable the UTA2 data ports to your host network: An FC host • 0c and 0d • **or** 0e and 0f A 10GbE • e0c and e0d • **or** e0e and e0f ⓘ You can connect one port pair as CNA and one port pair as FC, or you can connect both port pairs as CNA or both port pairs as FC.

Step	Perform on each controller module
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Option 3: Cable a two-node switchless cluster, Ethernet network configuration

Management network, Ethernet data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the cluster interconnect cable: • e0a to e0a • e0b to e0b
2	Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:

Step	Perform on each controller
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Option 4: Cable a switched cluster, Ethernet network configuration

Management network, Ethernet data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and the switches:

Step	Perform on each controller module
1	Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:
2	Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:

Step	Perform on each controller module
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Step 4: Cable controllers to drive shelves

You must cable the controllers to your shelves using the onboard storage ports. NetApp recommends MP-HA cabling for systems with external storage. If you have a SAS tape drive, you can use single-path cabling. If you have no external shelves, MP-HA cabling to internal drives is optional (not shown) if the SAS cables are ordered with the system.

Option 1: Cable storage on an HA pair with external drive shelves

You must cable the shelf-to-shelf connections, and then cable both controllers to the drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

Steps

1. Cable the HA pair with external drive shelves:

> The example uses DS224C. Cabling is similar with other supported drive shelves.

Step	Perform on each controller
1	Cable the shelf-to-shelf ports. • Port 3 on IOM A to port 1 on the IOM A on the shelf directly below. • Port 3 on IOM B to port 1 on the IOM B on the shelf directly below. mini-SAS HD to mini-SAS HD cables
2	Connect each node to IOM A in the stack. • Controller 1 port 0b to IOM A port 3 on last drive shelf in the stack. • Controller 2 port 0a to IOM A port 1 on the first drive shelf in the stack. mini-SAS HD to mini-SAS HD cables
3	Connect each node to IOM B in the stack • Controller 1 port 0a to IOM B port 1 on first drive shelf in the stack. • Controller 2 port 0b to IOM B port 3 on the last drive shelf in the stack. mini-SAS HD to mini-SAS HD cables

If you have more than one drive shelf stack, see the *Installation and Cabling Guide* for your drive shelf type.

Installing and cabling

2. To complete setting up your system, see Completing system setup and configuration

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Complete system setup if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Use the following animation to set one or more drive shelf IDs

   Setting drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

> Initial booting may take up to eight minutes.

4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:

a. Open File Explorer.
b. Click network in the left pane.
c. Right click and select refresh.
d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

> XXXXX is the system serial number for the target node.

System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

   ONTAP Configuration Guide

8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

   > See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console, and connect the console port on the controller using the console cable that came with your system.

c. Connect the laptop or console to the switch on the management subnet.

d. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.

2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.

If the management network has DHCP…	Then…
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

7. Verify the health of your system by running Config Advisor.
8. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A220 and FAS2700

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.

- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys - AFF A220 and FAS2700

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes` manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to back up the OKM information: `security key-manager backup show`

> Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

- Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. Shut down the impaired controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. Shut down the impaired controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager external sync`

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. You can safely shut down the controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the impaired controller - AFF A220 and FAS2700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.

If the impaired controller displays…	Then…
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A220 and FAS2700

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Replace the boot media

You must locate the boot media in the controller and follow the directions to replace it.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:

3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

4. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
5. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the var file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.

- If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.

- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired controller from the healthy controller during var file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.
     - dns_addr is the IP address of a name server on your network.
     - dns_domain is the Domain Name System (DNS) domain name.

If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

> Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

Boot the recovery image - AFF A220 and FAS2700

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.

d. Save your changes using the `savenv` command.

5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.
10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - AFF A220 and FAS2700

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:

```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.

b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

> If the `Restored` column = anything other than `yes`, contact Customer Support.

c. Wait 10 minutes for the key to synchronize across the cluster.

14. If you are running ONTAP 9.6 or later:

    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.

    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

    > If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.

15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.

If the console displays…	Then…
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.
   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A220 and FAS2700

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module - AFF A220 and FAS2700

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

- You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller.

+
ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

Steps

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run`
   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

      The output should display the caching module status as erased.
2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace a caching module

To replace a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the caching module at the rear of the controller module and remove it.

   a. Press the release tab.

   b. Remove the heatsink.

3. Gently pull the caching module straight out of the housing.
4. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
5. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

6. Reseat and push the heatsink down to engage the locking button on the caching module housing.

7. Close the controller module cover, as needed.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>)

appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`
4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

1. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation: **If your controller is in an HA pair**, perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* **Note:** If you disabled automatic giveback, re-enable it with the `storage failover modify` command. **If your controller is in a stand-alone configuration**, proceed to the next step. No action is required. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A220 and FAS2700

To replace the chassis, you must move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A220 and FAS2700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Controller is in a MetroCluster configuration

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Move and replace hardware - AFF A220 and FAS2700

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Move a power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

4. Use the cam handle to slide the power supply out of the system.

> When removing a power supply, always use two hands to support its weight.

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

> Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

> Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

Step 2: Remove the controller module

Remove the controller module or modules from the old chassis.

1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

2. Remove and set aside the cable management devices from the left and right sides of the controller module.

3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

4. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 3: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It click when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 4: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Repeat the preceding steps for the second controller module in the new chassis.
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Reinstall the blanking panel and then go to the next step.

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

      If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

   b. From the boot menu, select the option for Maintenance mode.

Restore and verify the configuration - AFF A220 and FAS2700

You must verify the HA state of the chassis and run System-Level diagnostics, switch back aggregates, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis HA-state`

      The value for HA-state can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. The next step depends on your system configuration.

If your system is in…	Then…
A stand-alone configuration	a. Exit Maintenance mode: `halt` b. Go to "Completing the replacement process.
An HA pair with a second controller module	Exit Maintenance mode: `halt` The LOADER prompt appears.

Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the controller to normal operation:

If your system is running ONTAP…	Then…
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If your system is running ONTAP…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - AFF A220 and FAS2700

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

  If this is the procedure you should use, note that the controller replacement procedure for a controller in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific

steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system's configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - AFF A220 and FAS2700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=_number_of_hours_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module..
Waiting for giveback…	Press Ctrl-C, and then respond `y`.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the controller module hardware - AFF A220 and FAS2700

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove controller module

To replace the controller module, you must first remove the old controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

6. Turn the controller module over and place it on a flat, stable surface.
7. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.

7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

Step 3: Move the boot media

You must locate the boot media and follow the directions to remove it from the old controller module and insert it in the new controller module.

1. Locate the boot media using the following illustration or the FRU map on the controller module:

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired

controller module to the corresponding slots in the replacement controller module.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

   > Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

   The number and placement of system DIMMs depends on the model of your system.

   The following illustration shows the location of system DIMMs:

4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

Make sure that the plug locks down onto the controller module.

Step 5: Move a caching module, if present

If your AFF A220 or FAS2700 system has a caching module, you need to move the caching module from the old controller module to the replacement controller module. The caching module is referred to as the “M.2 PCIe card” on the controller module label.

You must have the new controller module ready so that you can move the caching module directly from the old controller module to the corresponding slot in the new one. All other components in the storage system must be functioning properly; if not, you must contact technical support.

1. Locate the caching module at the rear of the controller module and remove it.

   a. Press the release tab.

   b. Remove the heatsink.

2. Gently pull the caching module straight out of the housing.
3. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Close the controller module cover, as needed.

Step 6: Install the controller

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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; you might damage the connectors. The controller begins to boot as soon as it is seated in the chassis. 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. Interrupt the boot process **only** after determining the correct timing: You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete. Only press `Ctrl-C` when you see the message `Press Ctrl-C for Boot Menu`. ⓘ If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Interrupt the boot process **only** after determining the correct timing: You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete. Only press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. f. From the boot menu, select the option for Maintenance mode.

Important: During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

    - `ha`
    - `mcc`
    - `mcc-2n`
    - `mccip`
    - `non-ha`

b. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device..
   - cna is a Converged Network Adapter or interface not connected to a network or storage device.
   - fcal is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - mem is system memory.
   - nic is a network interface card.
   - `nvram` is nonvolatile RAM.
   - `nvmem` is a hybrid of NVRAM and system memory.
   - `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`* *dev_name* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev` *`dev_name`* After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - AFF A220 and FAS2700

To complete the replacement procedure and restore your system to full operation, you must recable the storage, confirm disk reassignment, restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller. You must complete a series of tasks before restoring your system to full operation.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.

c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.

You must use the correct procedure for your configuration:

Controller redundancy	Then use this procedure…
HA pair	Verifying the system ID change on an HA system
Stand-alone	Manually reassigning the system ID on a stand-alone system in ONTAP
Two-node MetroCluster configuration	Manually reassigning the system ID on systems in a two-node MetroCluster configuration

Option 1: Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node` *`local-node-name`* `partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration content for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

Option 2: Manually reassign the system ID on a stand-alone system in ONTAP

In a stand-alone system, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems that are in a stand-alone configuration.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.
2. You must enter `Y` when prompted to override the system ID due to a system ID mismatch.
3. View the system IDs: `disk show -a`
4. You should make a note of the old system ID, which is displayed as part of the disk owner column.

   The following example shows the old system ID of 118073209:

```
*> disk show -a
Local System ID: 118065481

  DISK      OWNER                  POOL   SERIAL NUMBER  HOME
--------    -------------          -----  -------------  -------------
disk_name    system-1  (118073209)  Pool0  J8XJE9LC       system-1
(118073209)
disk_name    system-1  (118073209)  Pool0  J8Y478RC       system-1
(118073209)
.
.
.
```

5. Reassign disk ownership by using the system ID information obtained from the disk show command: `disk reassign -s old system ID disk reassign -s 118073209`
6. Verify that the disks were assigned correctly: `disk show -a`

   The disks belonging to the replacement node should show the new system ID. The following example now show the disks owned by system-1 the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK      OWNER                   POOL   SERIAL NUMBER  HOME
--------    -------------           -----  -------------  -------------
disk_name    system-1  (118065481)  Pool0  J8Y0TDZC       system-1
(118065481)
disk_name    system-1  (118065481)  Pool0  J8Y0TDZC       system-1
(118065481)
.
.
.
```

7. Boot the node: `boot_ontap`

Option 3: Manually reassign the system ID on systems in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering `Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid`,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

```
dr-group-id cluster         node                 node-systemid dr-
partner-systemid
 ----------- --------------------- -------------------- -------------
-------------------
 1           Cluster_A             Node_A_1             536872914
118073209
 1           Cluster_B             Node_B_1             118073209
536872914
 2 entries were displayed.
```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

```
Local System ID: 118065481
    ...
    ...
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                 POOL   SERIAL NUMBER  HOME
-------    -------------         -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:

a. Change to the advanced privilege level: `set -privilege advanced`

   You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

b. Verify that the coredumps are saved: `system node run -node local-node-name partner savecore`

   If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node local-node-name partner savecore -s command`.</info>.

c. Return to the admin privilege level: `set -privilege admin`

7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`

c. Return to the admin privilege level: `set -privilege admin`

Complete system restoration - AFF A220 and FAS2700

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

> The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption

functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and register the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A220 and FAS2700

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Steps

1. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
2. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

3. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

3. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
4. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:

a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.

b. Confirm that the NVMEM LED is no longer lit.

c. Reconnect the battery connector.

5. Return to Replace the DIMMs of this procedure to recheck the NVMEM LED.
6. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

7. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
8. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

9. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

10. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

    The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

    Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

11. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
12. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

13. Close the controller module cover.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. > If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF A220 and FAS2700

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - AFF A220 and FAS2700

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
5. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

6. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller

module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

Steps

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

3. Locate the NVMEM battery in the controller module.

4. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
5. Remove the battery from the controller module and set it aside.
6. Remove the replacement battery from its package.
7. Loop the battery cable around the cable channel on the side of the battery holder.
8. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
9. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
10. Plug the battery plug back into the controller module.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A220 and FAS2700

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

- Power supplies are auto-ranging.

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

5. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. Reconnect the power supply cabling:

   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

10. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

    The power supply LEDs are lit when the power supply comes online.

11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a two-node MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and set time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

AFF A250 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick steps - AFF A250

This section gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

- English: AFF A250 Installation and Setup Instructions
- Japanese: AFF A250 Systems Installation and Setup Instructions
- Chinese: AFF A250 Systems Installation and Setup Instructions

Videos - AFF A250

There are two videos - one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and Setup of an AFF A250

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed steps - AFF A250

This section gives detailed step-by-step instructions for installing an AFF A250 system.

Step 1: Prepare for installation

To install your AFF A250 system, you need to create an account and register the system. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the NetApp Hardware Universe (HWU) for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

> Customers with specific power requirements must check HWU for their configuration options.

What you need

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register (NetApp Product Registration) your system.
4. Download and install NetApp Downloads: Config Advisor on your laptop.
5. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the NetApp Hardware Universe to locate the cable and identify its use.

Type of cable…	Part number and length	Connector type	For…
25 GbE cable	X66240A-05 (112-00595), 0.5m; X66240-2 (112-00573), 2m		Cluster interconnect network
	X66240A-2 (112-00598), 2m; X66240A-5 (112-00600), 5m		Data
100 GbE cable	X66211-2 (112-00574), 2m; X66211-5 (112-00576), 5m		Storage
RJ-45 (order dependent)	Not applicable		Management network (BMC and wrench port) and Ethernet data (e0a and e0b)
Fibre Channel	X66250-2 (112-00342) 2m; X66250-5 (112-00344) 5m; X66250-15 (112-00346) 15m; X66250-30 (112-00347) 30m		
Micro-USB console cable	Not applicable		Console connection during software setup
Power cables	Not applicable		Powering up the system

6. Review the ONTAP Configuration Guide and collect the required information listed in that guide.

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

> You need to be aware of the safety concerns associated with the weight of the system.

3. Identify and manage cables because this system does not have a cable management device.
4. Place the bezel on the front of the system.

Step 3: Cable controllers

There is required cabling for your platform's cluster using the two-node switchless cluster method or the cluster interconnect network method. There is optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cable to a host network and storage.

Required cabling: Cable controllers to a cluster

Cable the controllers to a cluster by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster

The management, Fibre Channel, and data or host network ports on the controller modules are connected to switches. The cluster interconnect ports are cabled on both controller modules.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cable a two-node switchless cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the 25GbE cluster interconnect cable : • e0c to e0c • e0d to e0d
2	Cable the wrench ports to the management network switches with the RJ45 cables.
!	DO NOT plug in the power cords at this point.

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 2: Cable a switched cluster

All ports on the controllers are connected to switches; cluster interconnect, management, Fibre Channel, and data or host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cabling a switched cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to the 25 GbE cluster interconnect switches. • e0c • e0d
2	Cable the wrench ports to the management network switches with the RJ45 cables.
!	DO NOT plug in the power cords at this point.

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Optional cabling: Cable configuration-dependent options

You have configuration-dependent optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cabling to a host network and storage.

Option 1: Cable to a Fibre Channel host network

Fibre Channel ports on the controllers are connected to Fibre Channel host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Step	Perform on each controller module
1	Cable ports 2a through 2d to the FC host switches.
2	To perform other optional cabling, choose from: • Option 2: Cable to a 25GbE data or host network • Option 3: Cable the controllers to a single drive shelf
3	To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 2: Cable to a 25GbE data or host network

25GbE ports on the controllers are connected to 25GbE data or host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Step	Perform on each controller module
1	Cable ports e4a through e4d to the 10GbE host network switches.
2	To perform other optional cabling, choose from: • Option 1: Cable to a Fibre Channel host network • Option 3: Cable the controllers to a single drive shelf
3	To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 3: Cable the controllers to a single drive shelf

Cable each controller to the NSM modules on the NS224 drive shelf.

Before you begin

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

1. Use the animation (Cabling the controllers to a single NS224) or the step-by-step instructions to cable your controller modules to a single shelf.

Step	Perform on each controller module
1	Cable controller A to the shelf:
2	Cable controller B to the shelf:

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Step 4: Complete system setup and configuration

Complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Complete system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   The system begins to boot. Initial booting may take up to eight minutes.

2. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

3. Use the animation (Connecting your laptop to the Management switch) to connect your laptop to the Management switch.
4. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click **Network** in the left pane.
   c. Right-click and select **refresh**.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

5. Use System Manager guided setup to configure your system using the data you collected in the ONTAP Configuration Guide.
6. Verify the health of your system by running Config Advisor.
7. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Complete system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the laptop or console to the switch on the management subnet.

   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   The system begins to boot. Initial booting may take up to eight minutes.

3. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

4. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the ONTAP Configuration Guide.
5. Verify the health of your system by running Config Advisor.
6. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A250

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots.

Before you begin

You must have a USB flash drive, formatted to MBR/FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

About this task

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* node is the controller on which you are performing maintenance.
  - The *healthy* node is the HA partner of the impaired controller.

Check onboard encryption keys - AFF A250

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message`

`MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`,

you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. Shut down the impaired controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. Shut down the impaired controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager external sync`

     If the command fails, contact NetApp Support.

     mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. You can safely shut down the controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

     Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the controller - AFF A250

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Systems in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A250

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module - AFF A250

To access components inside the controller module, you must first remove the controller module from the system, and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.

2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.

Step 2: Replace the boot media

You locate the failed boot media in the controller module by removing the air duct on the controller module before you can replace the boot media.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not lose it.

You can use the following video or the tabulated steps to replace the boot media:

Replacing the boot media

1. Locate and replace the impaired boot media from the controller module.

1	Remove the screw securing the boot media to the motherboard in the controller module.
2	Lift the boot media out of the controller module.

2. Using the #1 magnetic screwdriver, remove the screw from the impaired boot media, and set it aside safely on the magnet.
3. Gently lift the impaired boot media directly out of the socket and set it aside.
4. Remove the replacement boot media from the antistatic shipping bag and align it into place on the controller module.
5. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed is without a boot image so you need to transfer a boot image using a USB flash drive.

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download

button.

  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.

- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
2. Download the service image to your work space on your laptop.
3. Unzip the service image.

   > If you are extracting the contents using Windows, do not use winzip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

   There are two folders in the unzipped service image file:

   - boot
   - efi

4. Copy the efi folder to the top directory on the USB flash drive.

   The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

5. Remove the USB flash drive from your laptop.
6. If you have not already done so, install the air duct.

7. Close the controller module cover and tighten the thumbscrew.

❶	Controller module cover
❷	Thumbscrew

8. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
9. Plug the power cable into the power supply and reinstall the power cable retainer.
10. Insert the USB flash drive into the USB slot on the controller module.

    Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

11. Push the controller module all the way into the chassis:
12. Place your index fingers through the finger holes from the inside of the latching mechanism.
13. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
14. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

    The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

    The controller module should be fully inserted and flush with the edges of the chassis.

15. 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.

16. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

    The system begins to boot and stops at the LOADER prompt.

17. Set your network connection type at the LOADER prompt:
    - If you are configuring DHCP: `ifconfig e0a -auto`

      > The target port you configure is the target port you use to communicate with the impaired controller from the healthy controller during var file system restore with a network connection. You can also use the e0M port in this command.

    - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
      - `filer_addr` is the IP address of the storage system.
      - `netmask` is the network mask of the management network that is connected to the HA partner.
      - `gateway` is the gateway for the network.

- `dns_addr` is the IP address of a name server on your network.
- `dns_domain` is the Domain Name System (DNS) domain name.

  If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

> Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

Boot the recovery image - AFF A250

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the `var` file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenvenvironment_variable_name changed_value` command.
   d. Save your changes using the `saveenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - AFF A250

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

   The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `storage failover show`-giveback` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.
7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.

- If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

  > If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A250

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A250

To replace the chassis, you must move the bezel, controller modules, and NVMe drives from the impaired chassis to the replacement chassis, and then remove the impaired chassis from the equipment rack or system cabinet and install the replacement chassis in its place.

About this task

- All other components in the system must be functioning properly; if not, you must contact technical support.
- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the bezel, NVMe drives, and controller modules to the new chassis, and that the replacement chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A250

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

> You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

Answer `y` when prompted.

Replace hardware - AFF A250

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

Use the following video or the tabulated steps to replace the chassis; it assumes the removal and replacement of the bezel:

Replacing the chassis

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run the diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

5. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - AFF A250

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:

   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

The value for HA-state can be one of the following:

- `ha`
- `mcc`
- `mccip`
- `non-ha`

b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test System** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement- AFF A250

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct

recovery procedure to determine whether you should use this procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller module - AFF A250

- 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 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).

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the controller module hardware - AFF A250

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

Use the following video or the tabulated steps to replace a controller module:

Replacing a controller module

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

❶	Thumbscrew
❷	Controller module cover.

7. Lift out the air duct cover.

Step 2: Move the power supply

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

1. Disconnect the power supply.
2. Open the power cable retainer, and then unplug the power cable from the power supply.
3. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab
2	Power supply

5. Move the power supply to the new controller module, and then install it.
6. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

Step 3: Move the fans

You must move the fans from the impaired controller module to the replacement module when replacing a failed controller module.

1. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan module

2. Move the fan module to the replacement controller module, and align the edges of the fan module with the opening in the controller module, and then slide the fan module in.
3. Repeat these steps for the remaining fan modules.

Step 4: Move the boot media

There is one boot media device in the AFF A250 under the air duct in the controller module. You must move it from the impaired controller module to the replacement controller module.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not lose it.

1. Locate and move the boot media from the impaired controller module to the replacement controller module.

1	Remove the screw securing the boot media to the motherboard in the impaired controller module.
2	Lift the boot media out of the impaired controller module.

a. Using the #1 magnetic screwdriver, remove the screw from the boot media, and set it aside safely on the magnet.
b. Gently lift the boot media directly out of the socket and align it into place in the replacement controller module.
c. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

Step 5: Move the DIMMs

To move the DIMMs, locate and move them from the impaired controller into the replacement controller and follow the specific sequence of steps.

+
image::../media/drw_a250_dimm_replace.png[]

+
NOTE: Install each DIMM into the same slot it occupied in the impaired controller module.

1. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.

> Hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

2. Locate the corresponding DIMM slot on the replacement controller module.
3. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

4. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
5. Repeat these steps for the remaining DIMM.

Step 6: Move a mezzanine card

To move a mezzanine card, you must remove the cabling and any QSFPs and SFPs from the ports, move the mezzanine card to the replacement controller, reinstall any QSFPs and SFPs onto the ports, and cable the ports.

1. Locate and move the mezzanine cards from your impaired controller module.

1	Remove screws on the face of the controller module.

❷	Loosen the screw in the controller module.
❸	Move the mezzanine card.

2. Unplug any cabling associated with the mezzanine card.

   Make sure that you label the cables so that you know where they came from.

   a. Remove any SFP or QSFP modules that might be in the mezzanine card and set it aside.
   b. Using the #1 magnetic screwdriver, remove the screws from the face of the impaired controller module and from the mezzanine card, and set them aside safely on the magnet.
   c. Gently lift the mezzanine card out of the socket and move it to the same position in the replacement controller.
   d. Gently align the mezzanine card into place in the replacement controller.
   e. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the replacement controller module and on the mezzanine card.

   > Do not apply force when tightening the screw on the mezzanine card; you might crack it.

3. Repeat these steps if there is another mezzanine card in the impaired controller module.
4. Insert the SFP or QSFP modules that were removed onto the mezzanine card.

Step 7: Move the NV battery

When replacing the controller module, you must move the NV battery from the impaired controller module to the replacement controller module.

1. Locate and move the NVMEM battery from your impaired controller module to the replacement controller module.

1	Squeeze the clip on the face of the battery plug.
2	Unplug the battery cable from the socket.
3	Grasp the battery and press the blue locking tab marked PUSH.
4	Lift the battery out of the holder and controller module.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Locate the corresponding NV battery holder on the replacement controller module and align the NV battery to the battery holder.
5. Insert the NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

Step 8: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustrations or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.

2. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

5. Insert the controller module into the chassis:
6. Ensure the latching mechanism arms are locked in the fully extended position.
7. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
8. Place your index fingers through the finger holes from the inside of the latching mechanism.
9. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
10. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching

mechanisms snap into place.

The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

The controller module should be fully inserted and flush with the edges of the chassis.

Restore and verify the system configuration - AFF A250

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - ha
   - mcc
   - mccip
   - non-ha

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test System** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

Recable the system and reassign disks - AFF A250

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                    Takeover
Node              Partner           Possible     State Description
------------      ------------      --------
-------------------------------------
node1             node2             false        System ID changed on
partner (Old:
                                                 151759755, New:
151759706), In takeover
node2             node1             -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

b. Save any coredumps: `system node run -node local-node-name partner savecore`

c. Wait for the `savecore`command to complete before issuing the giveback.

   You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration content for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node`

`show`

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* controller is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each controller is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each controller: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A250

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A250

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.

About this task

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.

Step 3: Replace a DIMM

To replace a DIMM, you must locate it in the controller module using the DIMM map label on top of the air duct or locating it using the LED next to the DIMM, and then replace it following the specific sequence of steps.

Use the following video or the tabulated steps to replace a DIMM:

Replacing a DIMM

1. Replace the impaired DIMM on your controller module.

   The DIMMs are in slot 3 or 1 on the motherboard. Slot 2 and 4 are left empty. Do not attempt to install DIMMs into these slots.

   The fault LED located on the board next to each DIMM blinks every two seconds.

2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
3. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.
4. Leave DIMM ejector tabs on the connector in the open position.
5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   > Hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

6. Insert the replacement DIMM squarely into the slot.

   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

7. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustrations or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.

2. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

3. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   ⓘ You will connect the rest of the cables to the controller module later in this procedure.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF A250

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a fan — AFF a250

To replace a fan, remove the failed fan module and replace it with a new fan module.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.

4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover

Step 3: Replace a fan

To replace a fan, remove the failed fan module and replace it with a new fan module.

Use the following video or the tabulated steps to replace a fan:

Replacing a fan

1. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
2. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan module

3. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace or install a mezzanine card - AFF A250

To replace a failed mezzanine card, you must remove the cables and any SFP or QSFP modules, replace the card, reinstall the SFP or QSFP modules and recable the cards. To install a new mezzanine card, you must have the appropriate cables and SFP or QSFP modules.

About this task

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

Remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module

cover.

1	Thumbscrew
2	Controller module cover.

Step 3: Replace or install a mezzanine card

To replace a mezzanine card, you must remove the impaired card and install the replacement card; to install a mezzanine card, you must remove the faceplate and install the new card.

Use the following video or the tabulated steps to replace a mezzanine card:

Replacing a mezzanine card

1. To replace a mezzanine card:
2. Locate and replace the impaired mezzanine card on your controller module.

1	Remove screws on the face of the controller module.
2	Loosen the screw in the controller module.
3	Remove the mezzanine card.

a. Unplug any cabling associated with the impaired mezzanine card.

   Make sure that you label the cables so that you know where they came from.

b. Remove any SFP or QSFP modules that might be in the impaired mezzanine card and set it aside.

c. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and set them aside safely on the magnet.

d. Using the #1 magnetic screwdriver, loosen the screw on the impaired mezzanine card.

e. Using the #1 magnetic screwdriver, gently lift the impaired mezzanine card directly out of the socket and set it aside.

f. Remove the replacement mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.

g. Gently align the replacement mezzanine card into place.

h. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

> Do not apply force when tightening the screw on the mezzanine card; you might crack it.

i. Insert any SFP or QSFP modules that were removed from the impaired mezzanine card to the replacement mezzanine card.

3. To install a mezzanine card:
4. You install a new mezzanine card if your system does not have one.
   a. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and the faceplate covering the mezzanine card slot, and set them aside safely on the magnet.
   b. Remove the mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.
   c. Gently align the mezzanine card into place.
   d. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

> Do not apply force when tightening the screw on the mezzanine card; you might crack it.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.

❶	Controller module cover
❷	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - AFF A250

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module.

Use the following video or the tabulated steps to replace the NVMEM battery:

Replacing the NVMEM battery

1. Locate and replace the impaired NVMEM battery on your controller module.

> It is recommended that you follow the illustrated instructions in the order listed.

1	Squeeze the clip on the face of the battery plug.
2	Unplug the battery cable from the socket.

❸	Grasp the battery and press the blue locking tab marked PUSH.
❹	Lift the battery out of the holder and controller module.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module and set it aside.
4. Remove the replacement NV battery from the antistatic shipping bag and align it to the battery holder.
5. Insert the replacement NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select Reboot from the menu to reboot the system.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a power supply - AFF A250

Replacing a power supply involves disconnecting the target power supply (PSU) from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting it to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- Power supplies are auto-ranging.

Use the following video or the tabulated steps to replace the power supply:

Replacing the power supply

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the red Fault LED on the power supply.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab
2	Power supply

5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

> To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

7. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A250

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 the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.

Step 3: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

Use the following video or the tabulated steps to replace the RTC battery:

Replacing the RTC battery

1. Locate the RTC battery between the heatsink and the midplane and remove it exactly as shown in the graphic.

1	Gently pull tab away from the battery housing. **Attention:** Pulling it away aggressively might displace the tab.
2	Lift the battery up. **Note:** Make a note of the polarity of the battery.
3	The battery should eject out.

The battery will be ejected out.

2. Remove the replacement battery from the antistatic shipping bag.
3. Locate the RTC battery holder between the heatsink and the midplane and insert it exactly as shown in the graphic.

1	With positive polarity face up, slide the battery under the tab of the battery housing.
2	Push the battery gently into place and make sure the tab secures it to the housing. + **CAUTION:** + Pushing it in aggressively might cause the battery to eject out again.

4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   f. Halt the controller at the LOADER prompt.

   The controller module should be fully inserted and flush with the edges of the chassis.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

AFF A300 System Documentation

Install and setup

Cluster configuration worksheet - AFF A300

You can use the worksheet to gather and record your site-specific IP addresses and other information required when configuring an ONTAP cluster.

Cluster Configuration Worksheet

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

Installation and setup PDF poster - AFF A300

You can use the PDF poster to install and set up your new system. The PDF poster provides step-by-step instructions with live links to additional content.

AFF A300 Installation and Setup Instructions

Installation and setup video - AFF A300

The following video shows end-to-end software configuration for systems running ONTAP 9.2.

AFF A300 Setup Video

Maintain

Boot media

Overview of boot media replacement - AFF A300

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys - AFF A300

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage`

```
failover modify -node local -auto-giveback-after-panic false
```

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes` manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers

display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        > Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`

   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.

- If no disks are shown, NSE is not configured.
- If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
     c. Shut down the impaired controller.
  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager onboard`

`sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

Shut down the impaired controller - AFF A300

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster configuration

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the boot media - AFF A300

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 2: Replace the boot media - AFF A300

You must locate the boot media in the controller and follow the directions to replace it.

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:

3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

4. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
5. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the var file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.

- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired controller from the healthy controller during var file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.

- dns_addr is the IP address of a name server on your network.
- dns_domain is the Domain Name System (DNS) domain name.

  If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

> Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

8. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:
   a. Boot to Maintenance mode: `boot_ontap maint`
   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t` *`initiator adapter_name`*
   c. Halt to return to Maintenance mode: `halt`

The changes will be implemented when the system is booted.

Boot the recovery image - AFF A300

The procedure for booting the impaired controller from the recovery image depends on whether the system is in a two-controller MetroCluster configuration.

Option 1: Most systems

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.

8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Controller is in a two-node MetroCluster

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. After the image is installed, start the restoration process:
   a. Press `n` when prompted to restore the backup configuration.
   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
   e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF A300

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - AFF A300

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

    > If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

    > If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.
18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.
19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.
   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.

- If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A300

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A300

To replace the chassis, you must move the power supplies, fans, and controller modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - - AFF A300

To replace the chassis, you must shutdown the controllers.

Option 1: Shut down the controller

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

> You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Controllers are in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace hardware - AFF A300

Move the power supplies, fans, and controller modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Move a power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Press down the release latch on the power supply cam handle, and then lower the cam handle to the fully open position to release the power supply from the mid plane.

1	Power supply
2	Cam handle release latch
3	Power and Fault LEDs
4	Cam handle

5	Power cable locking mechanism

4. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Push firmly on the power supply cam handle to seat it all the way into the chassis, and then push the cam handle to the closed position, making sure that the cam handle release latch clicks into its locked position.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

   Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

Step 2: Move a fan

Moving out a fan module when replacing the chassis involves a specific sequence of tasks.

1. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
2. Press down the release latch on the fan module cam handle, and then pull the cam handle downward.

   The fan module moves a little bit away from the chassis.

1	Cam handle
2	Fan module
3	Cam handle release latch
4	Fan module Attention LED

3. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

> The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

4. Set the fan module aside.
5. Repeat the preceding steps for any remaining fan modules.
6. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.
7. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

8. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

9. Repeat these steps for the remaining fan modules.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Step 3: Remove the controller module

To replace the chassis, you must remove the controller module or modules from the old chassis.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

6. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 4: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.

   If the system is in a system cabinet, you might need to remove the rear tie-down bracket.

2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. 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. Repeat the preceding steps if there is a second controller to install in the new chassis.
5. Complete the installation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. 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. Repeat the preceding steps for the second controller module in the new chassis.
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. 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. Reinstall the blanking panel and then go to the next step.

6. Connect the power supplies to different power sources, and then turn them on.
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 A300

You must verify the HA state of the chassis and run System-Level diagnostics, switch back aggregates, and return the failed part to NetApp, as described in the RMA

instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. The next step depends on your system configuration.

If your system is in…	Then…
A stand-alone configuration	a. Exit Maintenance mode: `halt` b. Go to Step 4: Return the failed part to NetApp.
An HA pair with a second controller module	Exit Maintenance mode: `halt` The LOADER prompt appears.

Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

> Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the controller to normal operation:

If your system is running ONTAP…	Then…
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If your system is running ONTAP…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - AFF A300

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

  If this is the procedure you should use, note that the controller replacement procedure for a controller in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific

steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system's configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- Any PCIe cards moved from the old controller module to the new controller module or added from existing customer site inventory must be supported by the replacement controller module.

  NetApp Hardware Universe

- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - AFF A300

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=_number_of_hours_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module..
Waiting for giveback…	Press Ctrl-C, and then respond `y`.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes

that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Open the controller module

To replace the controller module, you must first remove the old controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

6. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 2: Move the boot device

You must locate the boot media and follow the directions to remove it from the old controller and insert it in the new controller.

1. Locate the boot media using the following illustration or the FRU map on the controller module:

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

   > Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 3: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Open the CPU air duct and locate the NVMEM battery.

1	Battery lock tab
2	NVMEM battery pack

3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Remove the battery from the controller module and set it aside.

Step 4: Move the DIMMs

To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

4. Locate the slot where you are installing the DIMM.
5. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Repeat these steps for the remaining DIMMs.
7. Move the NVMEM battery to the replacement controller module.
8. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.

Step 5: Move a PCIe card

To move PCIe cards, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

You must have the new controller module ready so that you can move the PCIe cards directly from the old controller module to the corresponding slots in the new one.

1. Loosen the thumbscrew on the controller module side panel.
2. Swing the side panel off the controller module.

1	
Side panel	
2	
PCIe card	

3. Remove the PCIe card from the old controller module and set it aside.

   Make sure that you keep track of which slot the PCIe card was in.

4. Repeat the preceding step for the remaining PCIe cards in the old controller module.

5. Open the new controller module side panel, if necessary, slide off the PCIe card filler plate, as needed, and carefully install the PCIe card.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The card must be fully and evenly seated in the slot.

6. Repeat the preceding step for the remaining PCIe cards that you set aside.
7. Close the side panel and tighten the thumbscrew.

Step 6: Install the controller

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the CPU air duct.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	`The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.` a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Important: During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

Restore and verify the system configuration - AFF A300

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`
3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device..
   - cna is a Converged Network Adapter or interface not connected to a network or storage device.
   - fcal is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - mem is system memory.
   - nic is a network interface card.
   - `nvram` is nonvolatile RAM.
   - `nvmem` is a hybrid of NVRAM and system memory.
   - `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`* *dev_name* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev` *`dev_name`* After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - AFF A300

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must use the correct procedure for your configuration.

Option 1: Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* node and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* node is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired node, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

a. From the healthy node, give back the replaced node's storage: `storage failover giveback -ofnode replacement_node_name`

The *replacement* node takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

The disks belonging to the *replacement* node should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

Option 2: Manually reassign the system ID on systems in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering `Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid`,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

   ```
   dr-group-id cluster         node                 node-systemid dr-
   partner-systemid
    ----------- --------------------- -------------------- -------------
   -------------------
    1           Cluster_A             Node_A_1             536872914
   118073209
    1           Cluster_B             Node_B_1             118073209
   536872914
    2 entries were displayed.
   ```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

   ```
   Local System ID: 118065481
       ...
       ...
   ```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                 POOL   SERIAL NUMBER  HOME
-------    -------------         -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Verify that the coredumps are saved: `system node run -node` *`local-node-name`* `partner savecore`

      If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node` *`local-node-name`* `partner savecore -s command`.</info>.

   c. Return to the admin privilege level: `set -privilege admin`
7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

       You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).
    b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`
    c. Return to the admin privilege level: `set -privilege admin`

Complete system restoration - AFF A300

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement node in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My

Support section under Software licenses.

> The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and register the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A300

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

3. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
4. Unplug the battery:

   > The NVMEM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after Data ONTAP has successfully booted.

     a. Open the CPU air duct and locate the NVMEM battery.

1	NVMEM battery lock tab
2	NVMEM battery

b. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.

c. Wait a few seconds, and then plug the battery back into the socket.

5. Return to step 2 of this procedure to recheck the NVMEM LED.
6. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

7. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
8. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

9. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

10. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

    The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

    > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

11. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

12. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

13. Close the controller module cover.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

1. 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 system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.
3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.
5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6 (Two-node MetroCluster only): Switch back aggregates

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a fan - AFF A300

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press down the release latch on the fan module cam handle, and then pull the cam handle downward.

   The fan module moves a little bit away from the chassis.

1	Cam handle
2	Fan module
2	Cam handle release latch
4	Fan module Attention LED

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-

44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - AFF A300

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

1. If you are not already grounded, properly ground yourself.

2. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

3. Open the CPU air duct and locate the NVMEM battery.

❶	Battery lock tab
❷	NVMEM battery pack

4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Remove the replacement battery from its package.
6. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.
7. Close the CPU air duct.

   Make sure that the plug locks down to the socket.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

1. 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 system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

f. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.
3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.
5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode replacement_node_name` If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: (two-node MetroCluster only): Switch back aggregates

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe card - AFF A300

To replace a PCIe card, you must perform a specific sequence of tasks.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace a PCIe card

To replace a PCIe card, locate it within the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.

2. Loosen the thumbscrew on the controller module side panel.
3. Swing the side panel off the controller module.

1	Side panel
2	PCIe card

4. Remove the PCIe card from the controller module and set it aside.
5. Install the replacement PCIe card.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The PCIe card must be fully and evenly seated in the slot.

   > If you are installing a card in the bottom slot and cannot see the card socket well, remove the top card so that you can see the card socket, install the card, and then reinstall the card you removed from the top slot.

6. Close the side panel and tighten the thumbscrew.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. 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 system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis.

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. 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. If you have not already done so, reconnect the cables to the controller module. d. Bind the cables to the cable management device with the hook and loop strap.

If your system is in…	Then perform these steps…
A two-node MetroCluster configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. ⓘ 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. If you have not already done so, reconnect the cables to the controller module. d. Bind the cables to the cable management device with the hook and loop strap. e. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.

5. 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.

6. Return the controller to normal operation:

If your system is in…	Issue this command from the partner's console…
An HA pair	`storage failover giveback -ofnode` *`impaired_node_name`*
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.

7. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5 (two-node MetroCluster only): Switch back aggregate

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A300

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Press down the release latch on the power supply cam handle, and then lower the cam handle to the fully open position to release the power supply from the mid plane.

1	Power supply
2	Cam handle release latch
2	Power and Fault LEDs
4	Cam handle

❺	Power cable locking mechanism

5. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

8. Push firmly on the power supply cam handle to seat it all the way into the chassis, and then push the cam handle to the closed position, making sure that the cam handle release latch clicks into its locked position.
9. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

1. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

   The power supply LEDs are lit when the power supply comes online.

2. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A300

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 the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.

If the impaired controller…	Then…
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace the RTC Battery

To replace the RTC battery, locate them inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Tighten the thumbscrew on the cam handle on back of the controller module.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk

pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

AFF A320 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick guide - AFF A320

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A320 Systems Installation and Setup Instructions

Videos - AFF A320

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

NetApp video: AFF A320 Installation and setup

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - AFF A320

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Prepare for installation

To install your AFF A320 system, you need to create an account, register the system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
- A laptop or console with an RJ-45 connection and access to a Web browser

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register your system.

      NetApp Product Registration

4. Inventory and make a note of the number and types of cables you received.

The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
100 GbE cable (QSF(28)	X66211A-05 (112-00595), 0.5m X66211A-1 (112-00573), 1m X66211A-2 (112-00574), 2m X66211A-5 (112-00574), 5m		Storage, cluster interconnect/HA, and Ethernet data (order-dependent)
40 GbE cable	X66211A-1 (112-00573), 1m; X66211A-3 (112-00543),3m; X66211A-5 (112-00576), 5m		Storage, cluster interconnect/HA, and Ethernet data (order-dependent)
Ethernet cable - MPO	X66200-2 (112-00326), 2m X66250-5 (112-00328), 5m X66250-30 (112-00331), 30m		Ethernet cable (order dependent)
Optical cables	SR: X6553-R6 (112-00188), 2m X6554-R6 (112-00189), 15m X6537-R6 (112-00091), 30m LR: X66250-3 (112-00342), 2m X66260-5 (112-00344), 5m X66260-30 (112-00354), 30m		FC configurations (order-dependent)
RJ-45 (order dependent)	X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network
Micro-USB console cable	Not applicable		Console connection used during software setup if laptop or console does not support network discovery.

Type of cable…	Part number and length	Connector type	For…
Power cables	Not applicable		Powering up the system

5. Download and complete the *Cluster configuration worksheet*.

   Cluster Configuration Worksheet

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.

Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster

The optional data ports, optional NIC cards, and management ports on the controller modules are connected to switches. The cluster interconnect/HA ports are cabled on both controller modules.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

1. You can used the illustration or the step-by step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller module
1	Cable the cluster/HA ports to each other with the 100 GbE (QSFP28) cable: • e0a to e0a • e0d to e0d
2	If you are using your onboard ports for a data network connection, connect the 100GbE or 40Gbe cables to the appropriate data network switches: • e0g and e0h

Step	Perform on each controller module
3	If you are using your NIC cards for Ethernet or FC connections, connect the NIC card(s) to the appropriate switches:
4	Cable the e0M ports to the management network switches with the RJ45 cables.
!	DO NOT plug in the power cords at this point.

2. Cable your storage: Cabling controllers to drive shelves

Option 2: Cabling a switched cluster

The optional data ports, optional NIC cards, and management ports on the controller modules are connected to switches. The cluster interconnect/HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the

switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

1. You can used the illustration or the step-by step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller module
1	Cable the cluster/HA ports to the cluster/HA switch with the 100 GbE (QSFP28) cable: • e0a on both controllers to the cluster/HA switch • e0d on both controllers to the cluster/HA switch
2	If you are using your onboard ports for a data network connection, connect the 100GbE or 40Gbe cables to the appropriate data network switches: • e0g and e0h

Step	Perform on each controller module
3	If you are using your NIC cards for Ethernet or FC connections, connect the NIC card(s) to the appropriate switches:
4	Cable the e0M ports to the management network switches with the RJ45 cables.
!	DO NOT plug in the power cords at this point.

2. Cable your storage: Cabling controllers to drive shelves

Cable controllers to drive shelves

You must cable the controllers to your shelves using the onboard storage ports.

Option 1: Cable the controllers to a single drive shelf

You must cable each controller to the NSM modules on the NS224 drive shelf.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

1. You can use the illustration or the step-by-step instructions to cable your controllers to a single shelf.

Step	Perform on each controller module
1	Cable controller A to the shelf
2	Cable controller B to the shelf:

2. To complete setting up your system, see Completing system setup and configuration.

Option 2: Cable the controllers to two drive shelves

You must cable each controller to the NSM modules on both NS224 drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

1. You can use the following illustration or the written steps to cable your controllers to two drive shelves.

Step	Perform on each controller module
1	Cable controller A to the shelves:
2	Cable controller B to the shelves:

2. To complete setting up your system, see Completing system setup and configuration.

Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   The system begins to boot. Initial booting may take up to eight minutes

2. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

3. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

4. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

5. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

   ONTAP Configuration Guide

6. Verify the health of your system by running Config Advisor.
7. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet.

   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   The system begins to boot. Initial booting may take up to eight minutes

4. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.

If the management network has DHCP…	Then…
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

5. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

6. Verify the health of your system by running Config Advisor.
7. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A320

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys - AFF A320

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to go to the next section.

Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.
2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.

- If no disks are shown, NSE is not configured.
- If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. Shut down the impaired controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. Shut down the impaired controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard`

`sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

Shut down the node - AFF A320

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node. Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: System is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A320

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

a. Insert your forefinger into the latching mechanism on either side of the controller module.
b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

   The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

c. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
d. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 2: Replace the boot media

You must locate the boot media in the controller module, and then follow the directions to replace it.

1. Open the air duct and locate the boot media using the following illustration or the FRU map on the controller module:
2. Locate and remove the boot media from the controller module:

a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
b. Rotate the boot media up and gently pull the boot media out of the socket.
    1. Check the boot media to make sure that it is seated squarely and completely in the socket.

If necessary, remove the boot media and reseat it into the socket.

3. Lock the boot media in place:
    a. Rotate the boot media down toward the motherboard.
    b. Placing a finger at the end of the boot media by the blue button, push down on the boot media end to engage the blue locking button.
    c. While pushing down on the boot media, lift the blue locking button to lock the boot media in place.
4. Close the air duct.

Step 3: Transfer the boot image to the boot media using a USB flash drive

The replacement boot media that you installed does not have a boot image, so you need to transfer a boot image using a USB flash drive.

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
    - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
    - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.

- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.
  1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
     a. Download the service image to your work space on your laptop.
     b. Unzip the service image.

        > If you are extracting the contents using Windows, do not use winzip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

        There are two folders in the unzipped service image file:

        - boot
        - efi

     c. Copy the efi folder to the top directory on the USB flash drive.

        The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

     d. Remove the USB flash drive from your laptop.
  2. If you have not already done so, close the air duct.
  3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
  4. Reinstall the cable management device and recable the system, as needed.

     When recabling, remember to reinstall the media converters (SFPs or QSFPs) if they were removed.

  5. Plug the power cable into the power supply and reinstall the power cable retainer.
  6. Insert the USB flash drive into the USB slot on the controller module.

     Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

  7. Complete the reinstallation of the controller module:
     a. Make sure the latch arms are locked in the extended position.
     b. Using the latch arms, push the controller module into the chassis bay until it stops.

        > Do not push down on the latching mechanism at the top of the latch arms. Doing so with raise the locking mechanism and prohibit sliding the controller module into the chassis.

     c. Press down and hold the orange tabs on top of the latching mechanism.
     d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

        > The latching mechanism arms slide into the chassis.

        The controller module begins to boot as soon as it is fully seated in the chassis.

e. Release the latches to lock the controller module into place.

f. If you have not already done so, reinstall the cable management device.

8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the node to boot to LOADER.

9. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

10. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.

11. After the image is installed, start the restoration process:

    a. Record the IP address of the impaired node that is displayed on the screen.

    b. Press `y` when prompted to restore the backup configuration.

    c. Press `y` when prompted to overwrite /etc/ssh/ssh_host_dsa_key.

12. From the partner node in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address` *`impaired_node_IP_address`*

13. If the restore is successful, press `y` on the impaired node when prompted to use the restored copy?.

14. Press `y` when you see confirm backup procedure was successful, and then press `y` when prompted to reboot the node.

15. Verify that the environmental variables are set as expected.

    a. Take the node to the LOADER prompt.

       From the ONTAP prompt, you can issue the command system node halt -skip-lif-migration-before -shutdown true -ignore-quorum-warnings true -inhibit-takeover true.

    b. Check the environment variable settings with the `printenv` command.

    c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.

    d. Save your changes using the `savenv` command.

    e. Reboot the node.

16. With the rebooted impaired node displaying the `Waiting for giveback…` message, perform a giveback from the healthy node:

If your system is in…	Then…
An HA pair	After the impaired node is displaying the `Waiting for giveback…` message, perform a giveback from the healthy node: a. From the healthy node: `storage failover giveback -ofnode partner_node_name` The impaired node takes back its storage, finishes booting, and then reboots and is again taken over by the healthy node. ⓘ If the giveback is vetoed, you can consider overriding the vetoes. ONTAP 9 High-Availability Configuration Guide b. Monitor the progress of the giveback operation by using the `storage failover show-giveback` command. c. After the giveback operation is complete, confirm that the HA pair is healthy and that takeover is possible by using the `storage failover show` command. d. Restore automatic giveback if you disabled it using the storage failover modify command.

17. Exit advanced privilege level on the healthy node.

Boot the recovery image - AFF A320

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy node to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address impaired_node_IP_address` d. Return the node to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the node.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press **`y`**.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press **`y`**.

4. Ensure that the environmental variables are set as expected:
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment_variable_name changed_value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Post boot media replacement steps for OKM, NSE, and NVE

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner node. b. Confirm the target node is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner node.
8. Give back the node using the `storage failover giveback -fromnode local` command
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired node and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - AFF A320

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `storage failover show`-giveback` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.
7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.

- If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

  > If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A320

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A320

To replace the chassis, you must move the fans and controller modules from the impaired chassis to the new chassis of the same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the controller modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A320

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Move the fans, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:
   a. Insert your forefinger into the latching mechanism on either side of the controller module.
   b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

      The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

   c. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
   d. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.
6. Repeat these steps for the other controller module in the chassis.

Step 2: Move the fans

To move the fan modules to the replacement chassis when replacing the chassis, you must perform a specific sequence of tasks.

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

4. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

5. Set the fan module aside.
6. Repeat the preceding steps for any remaining fan modules.
7. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Repeat these steps for the remaining fan modules.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run the diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.

b. Using the latch arms, push the controller module into the chassis bay until it stops.
c. Press down and hold the orange tabs on top of the latching mechanism.
d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

> The latching mechanism arms slide into the chassis.

The controller module begins to boot as soon as it is fully seated in the chassis.

e. Release the latches to lock the controller module into place.
f. Recable the power supply.
g. If you have not already done so, reinstall the cable management device.
h. Interrupt the normal boot process by pressing `Ctrl-C`.

5. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - AFF A320

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

      - `ha`
      - `mcc`
      - `mccip`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - AFF A320

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- The healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

  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 A320

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following images or the written steps to remove the controller module from the chassis.

The following image shows removing the cables and cable management arms from the impaired controller module:

The following image shows removing the impaired controller module from the chassis:

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

a. Insert your forefinger into the latching mechanism on either side of the controller module.
b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

   The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

c. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
d. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 2: Move the power supplies

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

1. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the blue locking tab.

   > The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

2. Move the power supply to the new controller module, and then install it.
3. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

Step 3: Move the NVDIMM battery

To move the NVDIMM battery from the impaired controller module to the replacement controller module, you must perform a specific sequence of steps.

You can use the following illustration or the written steps to move the NVDIMM battery from the impaired controller module to the replacement controller module.

1. Locate the NVDIMM battery in the controller module.
2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Move the battery to the replacement controller module.
5. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.

> Do not plug the battery cable back into the motherboard until instructed to do so.

Step 4: Move the boot media

You must locate the boot media, and then follow the directions to remove it from the impaired controller module and insert it into the replacement controller module.

You can use the following illustration or the written steps to move the boot media from the impaired controller module to the replacement controller module.

1. Open the air duct and locate the boot media using the following illustration or the FRU map on the controller module:
2. Locate and remove the boot media from the controller module:
   a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
   b. Rotate the boot media up and gently pull the boot media out of the socket.
3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Placing a finger at the end of the boot media by the blue button, push down on the boot media end to engage the blue locking button.
   c. While pushing down on the boot media, lift the blue locking button to lock the boot media in place.

Step 5: Move the DIMMs

You need to locate the DIMMs, and then move them from the impaired controller module to the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

You can use the following illustrations or the written steps to move the DIMMs from the impaired controller module to the replacement controller module.

1. Locate the DIMMs on your controller module.

1	Air duct
2	• System DIMMs slots: 2,4, 7, 9, 13, 15, 18, and 20 • NVDIMM slot: 11 ⓘ The NVDIMM looks significantly different than system DIMMs.

2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Verify that the NVDIMM battery is not plugged into the new controller module.
4. Move the DIMMs from the impaired controller module to the replacement controller module:

   ⓘ Make sure that you install the each DIMM into the same slot it occupied in the impaired controller module.

   a. Eject the DIMM from its slot by slowly pushing apart the DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

      ⓘ Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

   b. Locate the corresponding DIMM slot on the replacement controller module.
   c. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

      The DIMMs fit tightly in the socket, but should go in easily. If not, realign the DIMM with the socket and reinsert it.

   d. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
   e. Repeat these substeps for the remaining DIMMs.
5. Plug the NVDIMM battery into the motherboard.

   Make sure that the plug locks down onto the controller module.

Step 6: Move the PCIe risers

You must move the PCIe risers, with the PCIe cards installed in them, from the impaired controller module to the replacement controller module.

You can use the following illustration or the written steps to move the PCIe risers from the impaired controller module to the replacement controller module.

1. Remove the cover over the PCIe risers by unscrewing the blue thumbscrew on the cover, slide the cover toward you, rotate the cover upward, lift it off the controller module, and then set it aside.
2. Remove the empty risers from the replacement controller module.
   a. Place your forefinger into the hole on the left side of the riser module and grasp the riser with your thumb.
   b. Lift the riser straight up and out of the bay, and then set it aside.
   c. Repeat these substeps for the second riser.
3. Move the PCIe risers from the impaired controller module to the same riser bays on the replacement controller module:
   a. Remove a riser from the impaired controller module and move it to the replacement controller module.
   b. Lower the riser straight into the bay, so that it is square with the bay and the pins of the riser slide into the guide holes at the rear of the bay.
   c. Seat the riser into the motherboard socket straight down into the socket by applying even downward pressure along the edges of the riser until it seats.

      The riser should seat smoothly with little resistence. Reseat the riser in the bay if you encounter significant resistance seating the riser into the socket.

   d. Repeat these substeps for the second riser.
   e. Reinstall the cover over the PCIe risers.

Step 7: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller

module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, close the air duct at the rear of the controller module and reinstall the cover over the PCIe cards.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.
   b. Using the latch arms, push the controller module into the chassis bay until it stops.
   c. Press down and hold the orange tabs on top of the latching mechanism.
   d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

      The latching mechanism arms slide into the chassis.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   e. Release the latches to lock the controller module into place.
   f. Recable the power supply.
   g. If you have not already done so, reinstall the cable management device.
   h. Interrupt the normal boot process by pressing `Ctrl-C`.

Restore and verify the system configuration - AFF A320

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system

settings as necessary.

Step 1: Set and verify 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 new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mccip`

- `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

Recable the system and reassign disks - AFF A320

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.

a. Download and install Config Advisor.
b. Enter the information for the target system, and then click Collect Data.
c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. Verify that the expected volumes are present for each controller: `vol show -node node-name`

8. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A320

To restore your system to full operation, you must restore the NetApp Storage Encryption

configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys

- Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A320

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

a. Insert your forefinger into the latching mechanism on either side of the controller module.
b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

   The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

c. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
d. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 3: Replace system DIMMs

Replacing a system DIMM involves identifying the target DIMM through the associated error message, locating the target DIMM using the FRU map on the air duct or the lit LED on the motherboard, and then replacing the DIMM.

1. Rotate the air duct to the open position.
2. Locate the DIMMs on your controller module.

1	Air duct
2	• System DIMMs slots: 2,4, 7, 9, 13, 15, 18, and 20 • NVDIMM slot: 11 ⓘ The NVDIMM looks significantly different than system DIMMs.

3. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
4. Eject the DIMM from its socket by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the socket.

   ⓘ Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

> Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
8. Close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

1. If you have not already done so, close the air duct at the rear of the controller module and reinstall the cover over the PCIe cards.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.
   b. Using the latch arms, push the controller module into the chassis bay until it stops.
   c. Press down and hold the orange tabs on top of the latching mechanism.
   d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

      > The latching mechanism arms slide into the chassis.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   e. Release the latches to lock the controller module into place.
   f. Recable the power supply.

g. If you have not already done so, reinstall the cable management device.

h. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 5: Run diagnostics

After you have replaced a system DIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Stress-Test system** from the displayed menu.
5. Select an option from the displayed sub-menu and run the test.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a fan module - AFF A320

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

> The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The Attention LED should not be lit after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Replace an NVDIMM - AFF A320

You must replace the NVDIMM in the controller module when your system registers that the flash lifetime is almost at an end or that the identified NVDIMM is not healthy in general; failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Shut down the controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

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.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

a. Insert your forefinger into the latching mechanism on either side of the controller module.
b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

a. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
b. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 3: Replace the NVDIMM

To replace the NVDIMM, you must locate it in the controller module using the NVDIMM map label on top of the air duct or locating it using the LED next to the NVDIMM, and then replace it following the specific sequence of steps.

> The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.

1. Open the air duct and then locate the NVDIMM in slot 11 on your controller module.

> The NVDIMM looks significantly different than system DIMMs.

2. Note the orientation of the NVDIMM in the socket so that you can insert the NVDIMM in the replacement controller module in the proper orientation.
3. Eject the NVDIMM from its slot by slowly pushing apart the two NVDIMM ejector tabs on either side of the NVDIMM, and then slide the NVDIMM out of the socket and set it aside.

   > Carefully hold the NVDIMM by the edges to avoid pressure on the components on the NVDIMM circuit board.

4. Remove the replacement NVDIMM from the antistatic shipping bag, hold the NVDIMM by the corners, and then align it to the slot.

   The notch among the pins on the NVDIMM should line up with the tab in the socket.

5. Locate the slot where you are installing the NVDIMM.
6. Insert the NVDIMM squarely into the slot.

   The NVDIMM fits tightly in the slot, but should go in easily. If not, realign the NVDIMM with the slot and reinsert it.

   > Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
8. Close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

1. If you have not already done so, close the air duct at the rear of the controller module and reinstall the cover over the PCIe cards.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.
   b. Using the latch arms, push the controller module into the chassis bay until it stops.
   c. Press down and hold the orange tabs on top of the latching mechanism.
   d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

> The latching mechanism arms slide into the chassis.

The controller module begins to boot as soon as it is fully seated in the chassis.

e. Release the latches to lock the controller module into place.
f. Recable the power supply.
g. If you have not already done so, reinstall the cable management device.
h. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 5: Run diagnostics

After you have replaced the NVDIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Select **NVDIMM Test** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVDIMM battery - AFF A320

To replace the NVDIMM battery, you must remove the controller module, remove the battery, replace the battery, and then reinstall the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

   a. Insert your forefinger into the latching mechanism on either side of the controller module.
   b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

   The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

   a. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
   b. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 3: Replace the NVDIMM battery

To replace the NVDIMM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module.

1. Open the air duct and locate the NVDIMM battery.
2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Remove the replacement battery from its package.
5. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.
6. Plug the battery plug back into the controller module, and then close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

1. If you have not already done so, close the air duct at the rear of the controller module and reinstall the cover over the PCIe cards.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.
   b. Using the latch arms, push the controller module into the chassis bay until it stops.
   c. Press down and hold the orange tabs on top of the latching mechanism.
   d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

   > The latching mechanism arms slide into the chassis.

   The controller module begins to boot as soon as it is fully seated in the chassis.

   e. Release the latches to lock the controller module into place.
   f. Recable the power supply.
   g. If you have not already done so, reinstall the cable management device.
   h. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe card - AFF A320

To replace a PCIe card, you must disconnect the cables from the cards, remove the SFP and QSFP modules from the cards before removing the riser, reinstall the riser, and then reinstall the SFP and QSFP modules before cabling the cards.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and,

if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message
MAINT=number_of_hours_downh
```

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

   a. Insert your forefinger into the latching mechanism on either side of the controller module.
   b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

   The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

   a. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
   b. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 3: Replace a PCIe card

You must remove the PCIe riser containing the failed PCIe card from the controller module, remove the failed PCIe card from the riser, install the replacement PCIe card in the riser, and then reinstall the riser into the controller module.

1. Remove the cover over the PCIe risers by unscrewing the blue thumbscrew on the cover, slide the cover toward you, rotate the cover upward, lift it off the controller module, and then set it aside.
2. Remove the riser with the failed PCIe card:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Place your forefinger into the hole on the left side of the riser module and grasp the riser with your thumb.
   c. Lift the riser straight out of the socket and set it aside.
3. Replace the card in the riser:
   a. Place the riser on a stable surface, and then turn the riser so that you can access the PCIe card.
   b. Place your thumbs just below the bottom edge of the PCIe card on either side of the socket, and then gently push up to release the card from the socket.
   c. Slide the card out of the riser and set it aside.
   d. Align the replacement card bezel with the edge of the riser and the outside edge of the card with the alignment guide on the left side of the riser.
   e. Gently slide the card until the card connector aligns with the riser socket, and then gently push the card down into the socket.
4. Reinstall the riser in the controller module:
   a. Align the riser over the opening so that the front edges of the riser are directly over the openings on the riser bay.
   b. Aligning the back edge of the riser so that the pins on the underside of the riser are over the holes in the sheet metal at the back riser bay.
   c. Apply even downward pressure to seat the riser straight down into the socket on the controller module.

d. Reinstall the PCIe riser cover on the controller module.

Sep 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

1. If you have not already done so, close the air duct at the rear of the controller module and reinstall the cover over the PCIe cards.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.
   b. Using the latch arms, push the controller module into the chassis bay until it stops.
   c. Press down and hold the orange tabs on top of the latching mechanism.
   d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

   > The latching mechanism arms slide into the chassis.

   The controller module begins to boot as soon as it is fully seated in the chassis.

   e. Release the latches to lock the controller module into place.
   f. Recable the power supply.
   g. If you have not already done so, reinstall the cable management device.
   h. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 5: Restore the controller module to operation

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a power supply - AFF A320

Replacing a power supply (PSU) involves disconnecting the target PSU from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting the replacement PSU to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- Power supplies are auto-ranging.

Figure 1. Steps

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Remove the power supply:
   a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
   b. Press the blue locking tab to release the power supply from the chassis.
   c. Using both hands, pull the power supply out of the chassis, and then set it aside.
5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Rotate the cam handle so that it is flush against the power supply.
7. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

8. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A320

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 controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Replace the RTC battery

You need to locate the RTC battery inside the controller module, and then follow the specific sequence of steps.

Step 3: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:

   a. Insert your forefinger into the latching mechanism on either side of the controller module.
   b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

   The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

a. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.

b. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

Step 4: Replace the RTC battery

1. Remove the PCIe cover.
   a. Unscrew the blue thumbscrew located above the onboard ports at the back of the controller module.
   b. Slide the cover toward you and rotate the cover upward.
   c. Remove the cover and set it aside.
2. Locate, remove, and then replace the RTC battery:
   a. Using the FRU map, locate the RTC battery on the controller module.
   b. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

   c. Remove the replacement battery from the antistatic shipping bag.

d. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.

3. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
4. Reinstall the PCIe cover on the controller module.

Step 5: Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. Make sure the latch arms are locked in the extended position.
   b. Using the latch arms, push the controller module into the chassis bay until it stops.

      > Do not push down on the latching mechanism at the top of the latch arms. Doing so with raise the locking mechanism and prohibit sliding the controller module into the chassis.

   c. Press down and hold the orange tabs on top of the latching mechanism.
   d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.

      > The latching mechanism arms slide into the chassis.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   e. Release the latches to lock the controller module into place.
   f. If you have not already done so, reinstall the cable management device.
   g. 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 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

AFF A400 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

Quick guide - AFF A400

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A400 Installation and Setup Instructions

Videos - AFF A400

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.

AFF A400 Installation and setup instructions AFF A400 Installation and setup instructions

Video two of two: Perform end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - AFF A400

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Step 1: Prepare for installation

To install your system, you need to create an account, register the system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

Before you begin

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
100 GbE cable (QSF(28)	X66211A-05 (112-00595), 0.5m X66211A-1 (112-00573), 1m X66211A-2 (112-00574), 2m X66211A-5 (112-00574), 5m		Storage, cluster interconnect/HA, and Ethernet data (order-dependent)
25 GbE cable (SFP28s)	X66240-2 (112-00598), 2m X66240-5 (112-00639), 5m		GbE network connection (order-dependent)
32 Gb FC (SFP+ Op)	X66250-2 (112-00342), 2m X66250-5 (112-00344), 5m X66250-15 (112-00346), 15m		FC network connection
Storage Cables	X66030A (112-00435), .5m X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		mini-SAS HD to mini-SAS HD cables (order-dependent)
Optical cables	X66250-2-N-C (112-00342)		16 Gb FC or 25GbE cables for mezzanine cards (order-dependent)
RJ-45 (order dependent)	X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network
Micro-USB console cable	Not applicable		Console connection used during software setup if laptop or console does not support network discovery.

Type of cable…	Part number and length	Connector type	For…
Power cables	Not applicable		Powering up the system

4. Review the *NetApp ONTAP Configuration Guide* and collect the required information listed in that guide.

   ONTAP Configuration Guide

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.

3. Attach cable management devices (as shown).

4. Place the bezel on the front of the system.

Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster

The optional data ports, optional NIC cards, and management ports on the controller modules are connected to switches. The cluster interconnect and HA ports are cabled on both controller modules.

You must have contacted your network administrator for information about connecting the system to the

switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Two-node switchless cluster cabling

2. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Option 2: Cable a switched cluster

The optional data ports, optional NIC cards, mezzanine cards, and management ports on the controller modules are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the

switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Switched cluster cabling

2. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Step 4: Cable controllers to drive shelves

You can cable either NSS224 or SAS shelves to you system.

Option 1: Cable the controllers to a single drive shelf

You must cable each controller to the NSM modules on the NS224 drive shelf.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the NS224 are up.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustration to cable your controllers to a single drive shelf.

   Cabling the controllers to one NS224 drive shelf

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Option 2: Cable the controllers to two drive shelves

You must cable each controller to the NSM modules on both NS224 drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the NS224 are up.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustration to cable your controllers to two drive shelves.

   Cabling controllers to two NS224 drive shelves

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Option 3: Cable the controllers to SAS drive shelves

You must cable each controller to the IOM modules on both SAS drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the DS224-C are down.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following illustration to cable your controllers to two drive shelves.

   Cabling the controllers to SAS drive shelves

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

1. Use the following animation to set one or more drive shelf IDs:

   If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

   Setting drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

4. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

5. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

6. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

ONTAP Configuration Guide

7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet .
   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

+
Setting drive shelf IDs

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   FAS8300 and FAS8700 shown.

   Power on the controllers

   Initial booting may take up to eight minutes.

2. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

3. 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

4. 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

5. Verify the health of your system by running Config Advisor.
6. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A400

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption - AFF A400

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.

4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.

- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the impaired controller - AFF A400

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller. Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster configuration

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node Metrocluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the boot media - AFF A400

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latches
2	Slide controller out of chassis

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 2: Replace the boot media

You must locate the boot media in the controller module (see the FRU map on the controller module), and then follow the directions to replace it.

Before you begin

Although the contents of the boot media is encrypted, it is a best practice to erase the contents of the boot media before replacing it. For more information, see the Statement of Volatility for your system on the NetApp Support Site.

> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the boot media.

Replacing the boot media

Steps

1. Open the air duct:

1	Locking tabs
2	Slide air duct toward back of controller
3	Rotate air duct up

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

2. Locate and remove the boot media from the controller module:

1	Press blue button
2	Rotate boot media up and remove from socket

a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
b. Rotate the boot media up and gently pull the boot media out of the socket.

3. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Placing a finger at the end of the boot media by the blue button, push down on the boot media end to engage the blue locking button.
   c. While pushing down on the boot media, lift the blue locking button to lock the boot media in place.
6. Close the air duct.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed does not have a boot image, so you need to transfer a boot image using a USB flash drive.

Before you begin

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the `var` file system.

Steps

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
   a. Download the service image to your work space on your laptop.
   b. Unzip the service image.

      > If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

      There are two folders in the unzipped service image file:

      - `boot`
      - `efi`

   c. Copy the `efi` folder to the top directory on the USB flash drive.

      The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

   d. Remove the USB flash drive from your laptop.
2. If you have not already done so, close the air duct.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
4. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs or QSFPs) if they were removed.

5. Plug the power cable into the power supply and reinstall the power cable retainer.
6. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

7. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. If you have not already done so, reinstall the cable management device.
8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then `halt` the controller to boot to LOADER.

9. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:

   a. Boot to Maintenance mode: `boot_ontap maint`
   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t` *`initiator adapter_name`*
   c. Halt to return to Maintenance mode: `halt`

   The changes will be implemented when the system is booted.

Boot the recovery image - AFF A400

The procedure for booting the impaired controller from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1: Most systems

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.

3. Restore the `var` file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

*If you see…	Then…*
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Controller is in a two-node MetroCluster

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. After the image is installed, start the restoration process:
   a. Press `n` when prompted to restore the backup configuration.
   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
   e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF A400

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the

configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - AFF A400

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.

6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


   ```
   ---------------------------BEGIN BACKUP---------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   ---------------------------END BACKUP---------------------------
   ```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show`

and `storage failover show-giveback` commands.

Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.

Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A400

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A400

To replace the chassis, you must move the fans and controller modules from the impaired chassis to the new chassis of the same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multinode cluster.

Shut down the controllers - AFF A400

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Shut down the controllers when replacing a chassis

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Shut down a controller in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace hardware - AFF A400

Move the fans, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move the fans

To move the fan modules to the replacement chassis when replacing the chassis, you must perform a specific sequence of tasks.

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

4. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   > The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

5. Set the fan module aside.
6. Repeat the preceding steps for any remaining fan modules.
7. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Repeat these steps for the remaining fan modules.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run the diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

4. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - AFF A400

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for *HA-state* can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - AFF A400

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

  If this is the procedure you should use, note that the controller replacement procedure for a controller in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.

- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement node* is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - AFF A400

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=_number_of_hours_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module..
Waiting for giveback…	Press Ctrl-C, and then respond `y`.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes

that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following , illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.
8. On the replacement controller module, open the air duct and remove the empty risers from the controller module using the animation, illustration, or the written steps:

   Removing the empty risers from the replacement controller module

   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
   c. Rotate the riser locking latch on the left side of riser 1 up and toward air duct, lift the riser up, and then set it aside.
   d. Repeat the previous step for the remaining risers.

Step 2: Move the power supplies

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

You can use the following animation, illustration, or the written steps to move the power supplies to the replacement controller module.

Moving the power supplies

1. Remove the power supply:

a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
b. Press the blue locking tab to release the power supply from the chassis.
c. Using both hands, pull the power supply out of the chassis, and then set it aside.

2. Move the power supply to the new controller module, and then install it.
3. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

4. Repeat the preceding steps for any remaining power supplies.

Step 3: Move the NVDIMM battery

To move the NVDIMM battery from the impaired controller module to the replacement controller module, you must perform a specific sequence of steps.

You can use the following animation, illustration, or the written steps to move the NVDIMM battery from the impaired controller module to the replacement controller module.

Moving the NVDIMM battery

1. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
2. Locate the NVDIMM battery in the controller module.
3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.

> Do not plug the battery cable back into the motherboard until instructed to do so.

Step 4: Move the boot media

You must locate the boot media, and then follow the directions to remove it from the impaired controller module and insert it into the replacement controller module.

You can use the following animation, illustration, or the written steps to move the boot media from the impaired controller module to the replacement controller module.

Moving the boot media

1. Locate and remove the boot media from the controller module:
   a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
   b. Rotate the boot media up and gently pull the boot media out of the socket.
2. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
3. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

4. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Press the blue locking button so that it is in the open position.
   c. Placing your fingers at the end of the boot media by the blue button, firmly push down on the boot media end to engage the blue locking button.

Step 5: Move the PCIe risers and mezzanine card

As part of the controller replacement process, you must move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

You can use the following animations, illustrations, or the written steps to move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

Moving PCIe riser 1 and 2 (left and middle risers):

Moving PCI risers 1 and 2

Moving the mezzanine card and riser 3 (right riser):

Moving the mezzanine card and riser 3

1. Move PCIe risers one and two from the impaired controller module to the replacement controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, and then move it to the replacement controller module.
   d. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins, push the riser squarely into the socket on the motherboard, and then rotate the latch down flush with the sheet metal on the riser.
   e. Repeat this step for riser number 2.
2. Remove riser number 3, remove the mezzanine card, and install both into the replacement controller

module:

a. Remove any SFP or QSFP modules that might be in the PCIe cards.
b. Rotate the riser locking latch on the left side of the riser up and toward air duct.

   The riser raises up slightly from the controller module.

c. Lift the riser up, and then set it aside on a stable, flat surface.
d. Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket, and then move it to the replacement controller module.
e. Install the mezzanine in the replacement controller and secure it with the thumbscrews.
f. Install the third riser in the replacement controller module.

Step 6: Move the DIMMs

You need to locate the DIMMs, and then move them from the impaired controller module to the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

You can use the following animation, illustration, or the written steps to move the DIMMs from the impaired controller module to the replacement controller module.

Moving the DIMMs

SLOTS
128GB
2, 4, 13, 15
256GB
2, 4, 7, 9 13, 15, 18, 20

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Verify that the NVDIMM battery is not plugged into the new controller module.
4. Move the DIMMs from the impaired controller module to the replacement controller module:

> Make sure that you install the each DIMM into the same slot it occupied in the impaired controller module.

   a. Eject the DIMM from its slot by slowly pushing apart the DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

b. Locate the corresponding DIMM slot on the replacement controller module.

c. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

   The DIMMs fit tightly in the socket, but should go in easily. If not, realign the DIMM with the socket and reinsert it.

d. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.

e. Repeat these substeps for the remaining DIMMs.

5. Plug the NVDIMM battery into the motherboard.

   Make sure that the plug locks down onto the controller module.

Step 7: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the replacement controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.
   g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

Restore and verify the system configuration - AFF A400

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.

2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt`

```
-node node_name
```

After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

Recable the system and reassign disks - AFF A400

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`

2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node *local-node-name* partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node *local-node-name* partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode *replacement_node_name*`

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

   The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node show`

   The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* controller is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each controller is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each controller: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A400

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

> The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A400

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace system DIMMs

Replacing a system DIMM involves identifying the target DIMM through the associated error message, locating the target DIMM using the FRU map on the air duct or the lit LED on the motherboard, and then replacing the DIMM.

You can use the following animation, illustration, or the written steps to replace a system DIMM.

> The animation and illustration show empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Replacing a system DIMM

The DIMMs are located in sockets 2, 4, 13, and 15. The NVDIMM is located in slot 11.

1. Open the air duct:

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
4. Eject the DIMM from its socket by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the socket.

   Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
8. Close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced a system DIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Select an option from the displayed sub-menu and run the test.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the

configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a fan module - AFF A400

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

You can use the following animation, illustration, or the written steps to hot-swap a fan module.

Replacing a fan

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   > The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The Attention LED should not be lit after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVDIMM battery - AFF A400

To replace the NVDIMM battery, you must remove the controller module, remove the battery, replace the battery, and then reinstall the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animations, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace the NVDIMM battery

To replace the NVDIMM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module. See the FRU map inside the controller module to locate the NVDIMM battery.

The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.

You can use the following animation, illustration, or the written steps to replace the NVDIMM battery.

Replacing the NVDIMM battery

1. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
2. Locate the NVDIMM battery in the controller module.
3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.

5. Remove the replacement battery from its package.
6. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.
7. Plug the battery plug back into the controller module, and then close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

   > If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an NVDIMM - AFF A400

You must replace the NVDIMM in the controller module when your system registers that the flash lifetime is almost at an end or that the identified NVDIMM is not healthy in general; failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data

from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message`

`MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animations, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.

3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace the NVDIMM

To replace the NVDIMM, you must locate it in the controller module using the FRU map on top of the air duct or locate the Attention LED using the FRU Map on the top of the slot 1 riser.

- The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.
- Although the contents of the NVDIMM is encrypted, it is a best practice to erase the contents of the NVDIMM before replacing it. For more information, see the Statement of Volatility on the NetApp Support Site.

> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the NVDIMM.

> The animation shows empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Replacing the NVDIMM

SLOTS
128GB
2, 4, 13, 15
256GB
2, 4, 7, 9 13, 15, 18, 20

1. Open the air duct and then locate the NVDIMM in slot 11 on your controller module.

   The NVDIMM looks significantly different than system DIMMs.

2. Eject the NVDIMM from its slot by slowly pushing apart the two NVDIMM ejector tabs on either side of the NVDIMM, and then slide the NVDIMM out of the socket and set it aside.

   Carefully hold the NVDIMM by the edges to avoid pressure on the components on the NVDIMM circuit board.

3. Remove the replacement NVDIMM from the antistatic shipping bag, hold the NVDIMM by the corners, and then align it to the slot.

   The notch among the pins on the NVDIMM should line up with the tab in the socket.

4. Locate the slot where you are installing the NVDIMM.

5. Insert the NVDIMM squarely into the slot.

   The NVDIMM fits tightly in the slot, but should go in easily. If not, realign the NVDIMM with the slot and reinsert it.

   > Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
7. Close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.
   g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced the NVDIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Select **NVDIMM Test** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.

- If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe or mezzanine card - AFF A400

To replace a PCIe or mezzanine card, you must disconnect the cables and any SFP and QSFP modules from the cards, replace the failed PCIe or mezzanine card, and then recable the cards.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.

If the impaired controller…	Then…
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animations, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace a PCIe card

To replace a PCIe card, you must locate the failed PCIe card, remove the riser that contains the card from the controller module, replace the card, and then reinstall the PCIe riser in the controller module.

You can use the following animation, illustration, or the written steps to replace a PCIe card.

Replacing a PCIe card

1. Remove the riser containing the card to be replaced:
   a. Open the air duct by pressing the locking tabs on the sides of the air duct, slide it toward the back of the controller module, and then rotate it to its completely open position.
   b. Remove any SFP or QSFP modules that might be in the PCIe cards.
   c. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   d. Lift the riser up straight up and set it aside on a stable flat surface,
2. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. For risers 2 and 3 only, swing the side panel up.
   d. Remove the PCIe card from the riser by gently pushing up on the bracket and lift the card straight out of the socket.
3. Install the replacement PCIe card in the riser by aligning the card with the socket, press the card into the socket and then close the side panel on the riser, if present.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The PCIe card must be fully and evenly seated in the slot.

   > If you are installing a card in the bottom slot and cannot see the card socket well, remove the top card so that you can see the card socket, install the card, and then reinstall the card you removed from the top slot.

4. Reinstall the riser:
    a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.
    b. Push the riser squarely into the socket on the motherboard.
    c. Rotate the latch down flush with the sheet metal on the riser.

Step 4: Replace the mezzanine card

The mezzanine card is located under riser number 3 (slots 4 and 5). You must remove that riser to access the mezzanine card, replace the mezzanine card, and then reinstall riser number 3. See the FRU map on the controller module for more information.

You can use the following animation, illustration, or the written steps to replace the mezzanine card.

Replacing the mezzanine card

1. Remove riser number 3 (slots 4 and 5):
    a. Open the air duct by pressing the locking tabs on the sides of the air duct, slide it toward the back of the controller module, and then rotate it to its completely open position.
    b. Remove any SFP or QSFP modules that might be in the PCIe cards.
    c. Rotate the riser locking latch on the left side of the riser up and toward air duct.

The riser raises up slightly from the controller module.

d. Lift the riser up, and then set it aside on a stable, flat surface.

2. Replace the mezzanine card:
   a. Remove any QSFP or SFP modules from the card.
   b. Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket and set it aside.
   c. Align the replacement mezzanine card over the socket and the guide pins and gently push the card into the socket.
   d. Tighten the thumbscrews on the mezzanine card.
3. Reinstall the riser:
   a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.
   b. Push the riser squarely into the socket on the motherboard.
   c. Rotate the latch down flush with the sheet metal on the riser.

Step 5: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.
   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
5. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
6. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 6: Restore the controller module to operation

To restore the controller, you must recable the system, give back the controller module, and then reenable automatic giveback.

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replacing a power supply - AFF A400

Replacing a power supply (PSU) involves disconnecting the target PSU from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting the replacement PSU to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

You can use the following animation, illustration, or the written steps to replace the power supply.

Replacing a power supply

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Remove the power supply:
   a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
   b. Press the blue locking tab to release the power supply from the chassis.
   c. Using both hands, pull the power supply out of the chassis, and then set it aside.
5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Rotate the cam handle so that it is flush against the power supply.
7. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

8. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A400

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animations, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace the RTC battery

You need to locate the RTC battery inside the controller module, and then follow the specific sequence of steps. See the FRU map inside the controller module for the location of the RTC battery.

You can use the following animation, illustration, or the written steps to replace the RTC battery.

Replacing the RTC battery

1. If you are not already grounded, properly ground yourself.
2. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
3. Locate, remove, and then replace the RTC battery:
   a. Using the FRU map, locate the RTC battery on the controller module.
   b. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

   > Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

   c. Remove the replacement battery from the antistatic shipping bag.
   d. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.

4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
5. Close the air duct.

Step 4: Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the installation of the controller module:
   a. Using the locking latches, firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

b. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

c. If you have not already done so, reinstall the cable management device.

d. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy controller with the `show date` command.

   b. At the LOADER prompt on the target controller, check the time and date.

   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.

   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.

   e. Confirm the date and time on the target controller.

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.

8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

AFF A700 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

Quick steps - AFF A700 and FAS9000

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A700 Installation and Setup Instructions

FAS9000 Installation and Setup Instructions

Video steps - AFF A700 and FAS9000

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and setup of an AFF A700 or FAS9000

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - AFF A700 and FAS9000

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Step 1: Prepare for installation

To install your system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

Before you begin

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
10 GbE network cable	X6566B-2-R6, (112-00299), 2m X6566B-3-R6, 112-00300, 3m X6566B-5-R6 , 112-00301, 5m		Network cable
40 GbE network cable 40 GbE cluster interconnect	X66100-1,112-00542, 1m X66100-3,112-00543, 3m		40 GbE network Cluster interconnect
100 GbE network cable 100 GbE storage cable	X66211A-05 (112-00595), 0.5m X66211A-1 (112-00573), 1m X66211A-2 (112-00574), 2m X66211A-5 (112-00574), 5m		Network cable Storage cable This cable applies to AFF A700 only.
Optical network cables (order dependent)	X6553-R6 (112-00188), 2m X6536-R6 (112-00090), 5m		FC host network
Cat 6, RJ-45 (order dependent)	Part numbers X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network and Ethernet data
Storage	X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		Storage
Micro-USB console cable	Not applicable		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	Not applicable		Powering up the system

4. Review the *NetApp ONTAP Confiuration Guide* and collect the required information listed in that guide.

   ONTAP Configuration Guide

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

You need to be aware of the safety concerns associated with the weight of the system.

The label on the left indicates an empty chassis, while the label on the right indicates a fully-populated system.

1. Attach cable management devices (as shown).

2. Place the bezel on the front of the system.

Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Two-node switchless cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Cabling a two-node switchless cluster

1. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Option 2: Switched cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Switched cluster cabling

1. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Step 4: Cable controllers to drive shelves

You can cable your new system to DS212C, DS224C, or NS224 shelves, depending on if it is an AFF or FAS system.

Option 1: Cable the controllers to DS212C or DS224C drive shelves

You must cable the shelf-to-shelf connections, and then cable both controllers to the DS212C or DS224C drive shelves.

The cables are inserted into the drive shelf with the pull-tabs facing down, while the other end of the cable is inserted into the controller storage modules with the pull-tabs up.

Steps

1. Use the following animations or illustrations to cable your drive shelves to your controllers.

> The examples use DS224C shelves. Cabling is similar with other supported SAS drive shelves.

   - Cabling SAS shelves in FAS9000, AFF A700, and ASA AFF A700, ONTAP 9.7 and earlier:

   Cabling SAS storage - ONTAP 9.7 and earlier

- Cabling SAS shelves in FAS9000, AFF A700, and ASA AFF A700, ONTAP 9.8 and later:

Cabling SAS storage - ONTAP 9.8 and later

If you have more than one drive shelf stack, see the *Installation and Cabling Guide* for your drive shelf type.

Install and cable shelves for a new system installation - shelves with IOM12 modules

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Option 2: Cable the controllers to a single NS224 drive shelf in AFF A700 and ASA AFF A700 systems running ONTAP 9.8 and later only

You must cable each controller to the NSM modules on the NS224 drive shelf on an AFF A700 or ASA AFF A700 running system ONTAP 9.8 or later.

- This task applies to AFF A700 and ASA AFF A700 running ONTAP 9.8 or later only.

- The systems must have at least one X91148A module installed in slots 3 and/or 7 for each controller. The animation or illustrations show this module installed in both slots 3 and 7.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustrations to cable your controllers with two X91148A storage modules to a single NS224 drive shelf, or use the diagram to cable your controllers with one X91148A storage module to a single NS224 drive shelf.

   Cabling a single NS224 shelf - ONTAP 9.8 and later

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Option 3: Cable the controllers to two NS224 drive shelves in AFF A700 and ASA AFF A700 systems running ONTAP 9.8 and later only

You must cable each controller to the NSM modules on the NS224 drive shelves on an AFF A700 or ASA AFF A700 running system ONTAP 9.8 or later.

- This task applies to AFF A700 and ASA AFF A700 running ONTAP 9.8 or later only.
- The systems must have two X91148A modules, per controller, installed in slots 3 and 7.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustrations to cable your controllers to two NS224 drive shelves.

   Cabling two NS224 shelves - ONTAP 9.8 and later

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Use the following animation to set one or more drive shelf IDs:

   If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

   Setting SAS or NVMe drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

   Turn on the power to the controllers

   > Initial booting may take up to eight minutes.

4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

      > XXXXX is the system serial number for the target node.

   System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the *NetApp*

ONTAP Configuration Guide.

ONTAP Configuration Guide

8. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

9. Verify the health of your system by running Config Advisor.
10. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet .

   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

Setting SAS or NVMe drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

   Turn on the power to the controllers

   Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

8. Verify the health of your system by running Config Advisor.

9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A700 and FAS9000

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz`.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair does not require connection to a network to restore the `var` file system. The HA pair in a single chassis has an internal e0S connection, which is used to transfer `var` config between them.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.

2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <Ino-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <Ino-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <Ino-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired node is part of an HA configuration, disable automatic giveback from the healthy node: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled,

you need to complete some other additional steps.

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

   c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.
   b. If the `Restored` column displays anything other than `yes`:
      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

> Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

- Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

b. Enter the command to display the key management information: `security key-manager onboard show-backup`

c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the impaired controller - AFF A700 and FAS9000

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.
NOTE: Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A700 and FAS9000

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

1	Controller module cover locking button

Step 2: Replace the boot media

Locate the boot media using the following illustration or the FRU map on the controller module:

❶	Press release tab
❷	Boot media

1. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

   > Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

2. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
3. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

4. Push the boot media down to engage the locking button on the boot media housing.
5. Reinstall the controller module lid by aligning the pins on the lid with the slots on the motherboard carrier, and then slide the lid into place.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the `var` file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the `var` file system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Recable the controller module, as needed.
3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, and then push the cam

handle to the closed position.

The node begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the node to boot to LOADER.

6. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired node from the healthy node during `var` file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.
     - dns_addr is the IP address of a name server on your network.
     - dns_domain is the Domain Name System (DNS) domain name.

       If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

     > Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

7. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:

   a. Boot to Maintenance mode: `boot_ontap maint`
   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t` *`initiator adapter_name`*
   c. Halt to return to Maintenance mode: `halt`

   The changes will be implemented when the system is booted.

Boot the recovery image - AFF A700 and FAS9000

The procedure for booting the impaired node from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1 Boot the recovery image in most systems

You must boot the ONTAP image from the USB drive, restore the file system, and verify

the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the `var` file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy node to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the node to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the node.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

*If you see…	Then…*
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner node. b. Confirm the target node is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner node.
8. Give back the node using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired node and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Boot the recovery image in a two-node MetroCluster configuration

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. After the image is installed, start the restoration process:
   a. Press `n` when prompted to restore the backup configuration.
   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
   a. Take the node to the LOADER prompt.

b. Check the environment variable settings with the `printenv` command.

c. If an environment variable is not set as expected, modify it with the `setenv environment-variable-name changed-value` command.

d. Save your changes using the `savenv` command.

e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF A700 and FAS9000

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - AFF A700 and FAS9000

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int`

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A700 and FAS9000

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module or add/replace a core dump module - AFF A700 and FAS9000

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation. If AutoSupport is not enabled, you can locate the failed caching module by the fault LED on the front of the module. You can also add or replace the 1TB, X9170A core dump module, which is required if you are installing NS224 drive shelves in an AFF A700 system.

Before you begin

- You must replace the failed component with a replacement FRU component you received from your provider.
- For instructions about hot swapping the caching module, see Hot-swapping a caching module.
- When removing, replacing, or adding caching or core dump modules, the target node must be halted to the LOADER.
- AFF A700 supports the 1TB core dump module, X9170A, which is required if you are adding NS224 drive shelves.
- The core dump modules can be installed in slots 6-1 and 6-2. The recommended best practice is to install the module in slot 6-1.
- The X9170A core dump module is not hot-swappable.

Step 1: Shutting down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace or add a caching module

The NVMe SSD Flash Cache modules (FlashCache or caching modules) are separate modules. They are located in the front of the NVRAM module. To replace or add a caching module, locate it on the rear of the system on slot 6, and then follow the specific sequence of steps to replace it.

Before you begin

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The target node must be at the LOADER prompt before adding or replacing the caching module.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.
3. Remove the caching module:

> If you are adding another caching module to your system, remove the blank module and go to the next step.

1	Orange release button.
2	Caching module cam handle.

a. Press the orange release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

   Be sure to support the caching module as you remove it from the NVRAM10 module.

4. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM10 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

Step 3: Add or replace an X9170A core dump module

The 1TB cache core dump, X9170A, is only used in the AFF A700 systems. The core dump module cannot be hot-swapped. The core dump module typically is located in the

front of the NVRAM module in slot 6-1 in the rear of the system. To replace or add the core dump module, locate slot 6-1, and then follow the specific sequence of steps to add or replace it.

Before you begin

- Your system must be running ONTAP 9.8 or later in order to add a core dump module.
- The X9170A core dump module is not hot-swappable.
- The target node must be at the LOADER prompt before adding or replacing the code dump module.
- You must have received two X9170 core dump modules; one for each controller.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you are replacing a failed core dump module, locate and remove it:

1	Orange release button.
2	Core dump module cam handle.

a. Locate the failed module by the amber Attention LED on the front of the module.

b. Press the orange release button on the front of the core dump module.

> Do not use the numbered and lettered I/O cam latch to eject the core dump module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the core dump module.

c. Rotate the cam handle until the core dump module begins to slide out of the NVRAM10 module.
d. Gently pull the cam handle straight toward you to remove the core dump module from the NVRAM10 module and set it aside.

   Be sure to support the core dump module as you remove it from the NVRAM10 module.

3. Install the core dump module:
   a. If you are installing a new core dump module, remove the blank module from slot 6-1.
   b. Align the edges of the core dump module with the opening in the NVRAM10 module.
   c. Gently push the core dump module into the bay until the cam handle engages.
   d. Rotate the cam handle until it locks into place.

Step 4: Reboot the controller after FRU replacement

After you replace the FRU, you must reboot the controller module.

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a caching module - AFF A700 and FAS9000

The NVMe SSD FlashCache modules (FlashCache or caching modules) are located in the front of the NVRAM10 module in Slot 6 of FAS9000 systems only. Beginning with ONTAP 9.4, you can hot-swap the caching module of the same capacity from the same or different supported vendor.

Before you begin

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.
3. Prepare the caching module slot for replacement as follows:

   a. For ONTAP 9.7 and earlier:

      i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

      ii. In admin privilege level, prepare the target NVMe slot for replacement, responding `y` when prompted whether to continue: `system controller slot module replace -node` *`node_name -slot slot_number`* The following command prepares slot 6-2 on node1 for replacement, and displays a message that it is safe to replace:

```
::> system controller slot module replace -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node node1 will be powered
off for replacement.
Do you want to continue? (y|n): `y`

The module has been successfully powered off.  It can now be
safely replaced.
After the replacement module is inserted, use the "system
controller slot module insert" command to place the module into
service.
```

iii. Display the slot status with the system controller slot module show command.

The NVMe slot status displays waiting-for-replacement in the screen output for the caching module that needs replacing.

b. For ONTAP 9.8 and later:

i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

ii. In admin privilege level, prepare the target NVMe slot for removal, responding `y` when prompted whether to continue: `system controller slot module remove -node node_name -slot slot_number` The following command prepares slot 6-2 on node1 for removal, and displays a message that it is safe to remove:

```
::> system controller slot module remove -node node1 -slot 6-2

Warning: SSD module in slot 6-2 of the node node1 will be powered
off for removal.
Do you want to continue? (y|n): `y`

The module has been successfully removed from service and powered
off. It can now be safely removed.
```

iii. Display the slot status with the `system controller slot module show` command.

The NVMe slot status displays `powered-off` in the screen output for the caching module that needs replacing.

See the Command man pages for your version of ONTAP for more details.

4. Remove the caching module:

1	Orange release button.
2	Caching module cam handle.

a. Press the orange release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

   Be sure to support the caching module as you remove it from the NVRAM10 module.

5. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM10 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

6. Bring the replacement caching module online by using the `system controller slot module insert` command as follows:

   The following command prepares slot 6-2 on node1 for power-on, and displays a message that it is

powered on:

```
::> system controller slot module insert -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node localhost will be powered
on and initialized.
Do you want to continue? (y|n): `y`

The module has been successfully powered on, initialized and placed into
service.
```

7. Verify the slot status using the `system controller slot module show` command.

   Make sure that command output reports status for slot 6-1 or 6-2 as `powered-on` and ready for operation.

8. Verify that the replacement caching module is online and recognized, and then visually confirm that the amber attention LED is not lit: `sysconfig -av slot_number`

   > If you replace the caching module with a caching module from a different vendor, the new vendor name is displayed in the command output.

9. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A700 and FAS9000

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A700 and FAS9000

To replace the chassis, you must shutdown the controllers.

Option 1: Shut down the controllers

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Shut down a node in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Move and replace hardware - AFF A700 and FAS9000

Move the fans, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the power supplies

Steps

Removing the power supplies when replacing a chassis involves turning off, disconnecting, and then removing the power supply from the old chassis.

1. If you are not already grounded, properly ground yourself.

2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.

> When removing a power supply, always use two hands to support its weight.

1	Locking button

4. Repeat the preceding steps for any remaining power supplies.

Step 2: Remove the fans

To remove the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

Steps

1. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
2. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

1	Orange release button

3. Set the fan module aside.
4. Repeat the preceding steps for any remaining fan modules.

Step 3: Remove the controller module

To replace the chassis, you must remove the controller module or modules from the old chassis.

Steps

1. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
2. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

3. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

4. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 4: Remove the I/O modules

Steps

To remove I/O modules from the old chassis, including the NVRAM modules, follow the specific sequence of steps. You do not have to remove the FlashCache module from the NVRAM module when moving it to a new chassis.

1. Unplug any cabling associated with the target I/O module.

   Make sure that you label the cables so that you know where they came from.

2. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

3. Set the I/O module aside.
4. Repeat the preceding step for the remaining I/O modules in the old chassis.

Step 5: Remove the De-stage Controller Power Module

Steps

You must remove the de-stage controller power modules from the old chassis in preparation for installing the replacement chassis.

1. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.

1	DCPM module orange locking button

2. Set the DCPM module aside in a safe place and repeat this step for the remaining DCPM module.

Step 6: Replace a chassis from within the equipment rack or system cabinet

Steps

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.

   If the system is in a system cabinet, you might need to remove the rear tie-down bracket.

2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.

5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. Secure the rear of the chassis to the equipment rack or system cabinet.
8. If you are using the cable management brackets, remove them from the old chassis, and then install them on the replacement chassis.
9. If you have not already done so, install the bezel.

Step 7: Move the USB LED module to the new chassis

Steps

Once the new chassis is installed into the rack or cabinet, you must move the USB LED module from the old chassis to the new chassis.

1. Locate the USB LED module on the front of the old chassis, directly under the power supply bays.
2. Press the black locking button on the right side of the module to release the module from the chassis, and then slide it out of the old chassis.
3. Align the edges of the module with the USB LED bay at the bottom-front of the replacement chassis, and gently push the module all the way into the chassis until it clicks into place.

Step 8: Install the de-stage controller power module when replacing the chassis

Steps

Once the replacement chassis is installed into the rack or system cabinet, you must reinstall the de-stage controller power modules into it.

1. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.

   > The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

2. Repeat this step for the remaining DCPM module.

Step 9: Install fans into the chassis

Steps

To install the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

1. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

   When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

2. Repeat these steps for the remaining fan modules.
3. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Step 10: Install I/O modules

Steps

To install I/O modules, including the NVRAM/FlashCache modules from the old chassis, follow the specific sequence of steps.

You must have the chassis installed so that you can install the I/O modules into the corresponding slots in the new chassis.

1. After the replacement chassis is installed in the rack or cabinet, install the I/O modules into their corresponding slots in the replacement chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage, and then push the I/O cam latch all the way up to lock the module in place.
2. Recable the I/O module, as needed.
3. Repeat the preceding step for the remaining I/O modules that you set aside.

> If the old chassis has blank I/O panels, move them to the replacement chassis at this time.

Step 11: Install the power supplies

Steps

Installing the power supplies when replacing a chassis involves installing the power supplies into the replacement chassis, and connecting to the power source.

1. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

   The power supplies are keyed and can only be installed one way.

   > Do not use excessive force when sliding the power supply into the system. You can damage the connector.

2. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

   > Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

3. Repeat the preceding steps for any remaining power supplies.

Step 12: Install the controller

Steps

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.

3. Connect the power supplies to different power sources, and then turn them on.
4. With the cam handle in the open position, slide the controller module into the chassis and firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle until it clicks into the locked position.

   > Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.

   The controller module begins to boot as soon as it is fully seated in the chassis.

5. Repeat the preceding steps to install the second controller into the new chassis.
6. Boot each node to Maintenance mode:
   a. As each node starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

      > If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

   b. From the boot menu, select the option for Maintenance mode.

Complete the restoration and replacement process - AFF A700 and FAS9000

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for `HA-state` can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.
4. Exit Maintenance mode: `halt`

   The LOADER prompt appears.

Step 2: Running system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the node boots to Maintenance mode, halt the node: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second node if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the node to normal operation:
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true` `node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - AFF A700 and FAS9000

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is a FlexArray system or has a V_StorageAttach license, you must refer to the additional required steps before performing this procedure.
- If your system is in an HA pair, the healthy node must be able to take over the node that is being replaced (referred to in this procedure as the “impaired node”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

If this is the procedure you should use, note that the controller replacement procedure for a node in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired node to the *replacement* node so that the *replacement* node will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* node is the node that is being replaced.
  - The *replacement* node is the new node that is replacing the impaired node.
  - The *healthy* node is the surviving node.
- You must always capture the node's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

To replace the controller module hardware, you must remove the impaired node, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

❶
Cam handle release button
❷
Cam handle

1. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

2. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

❶
Controller module cover locking button

Step 2: Move the boot media

You must locate the boot media and follow the directions to remove it from the old controller and insert it in the new controller.

Steps

1. Lift the black air duct at the back of the controller module and then locate the boot media using the following illustration or the FRU map on the controller module:

1	
Press release tab	
2	
Boot media	

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 3: Move the system DIMMs

To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

1	DIMM ejector tabs

❷	
DIMM	

5. Locate the slot where you are installing the DIMM.
6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

8. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
9. Repeat these steps for the remaining DIMMs.

Step 4: Install the controller

After you install the components into the controller module, you must install the controller module back into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
   e. Select the option to boot to Maintenance mode from the displayed menu.

Restore and verify the system configuration - AFF A700 and FAS9000

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`

     a. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device.
   - `cna` is a Converged Network Adapter or interface not connected to a network or storage device.
   - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - `mem` is system memory.

- `nic` is a network interface card.
- `nvram` is nonvolatile RAM.
- `nvmem` is a hybrid of NVRAM and system memory.
- `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev _dev_name` `dev_name` can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` + `-selection only` disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev dev_name` After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev dev_name -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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` `-selection only` disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the node: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The node displays the LOADER prompt. d. Boot the node from the LOADER prompt: `bye` e. Return the node to normal operation:
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the `storage failover modify` command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Recable the system and reassign disks - AFF A700 and FAS9000

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* node and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* node is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired node, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                      Takeover
Node               Partner            Possible     State Description
------------       ------------       --------
-------------------------------------
node1              node2              false        System ID changed on
partner (Old:
                                                     151759755, New:
151759706), In takeover
node2              node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt

appears (*>).

b. Save any coredumps: `system node run -node local-node-name partner savecore`

c. Wait for the `savecore`command to complete before issuing the giveback.

   You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

   a. From the healthy node, give back the replaced node's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* node takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration Guide for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* node should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the node: `metrocluster node show`

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each node will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the node is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a node on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* node is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each node is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each node: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A700 and FAS9000

To complete the replacement procedure and restore your system to full operation, you must recable the storage, restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller. You must complete a series of tasks before restoring your system to full operation.

Step 1: Install licenses for the replacement node in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

If the node is in a MetroCluster configuration and all nodes at a site have been replaced, license keys must be installed on the *replacement* node or nodes prior to switchback.

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   NetApp Support

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

Steps

1. Install each license key: `system license add -license-code license-key, license-key...`
2. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restoring Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verifying LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.

3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4 (MetroCluster only): Switching back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a de-stage controller power module (DCPM) - AFF A700 and FAS9000

To hot-swap a de-stage controller power module (DCPM), which contains the NVRAM10 battery, you must locate the failed DCPM module, remove it from the chassis, and install the replacement DCPM module.

You must have a replacement DCPM module in-hand before removing the failed module from the chassis and it must be replaced within five minutes of removal. Once the DCPM module is removed from the chassis, there is no shutdown protection for the controller module that owns the DCPM module, other than failover to the other controller module.

Replacing the DCPM module

To replace the DCPM module in your system, you must remove the failed DCPM module from the system and then replace it with a new DCPM module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel on the front of the system and set it aside.
3. Locate the failed DCPM module in the front of the system by looking for the Attention LED on the module.

   The LED will be steady amber if the module is faulty.

> The DCPM module must be replaced in the chassis within five minutes of removal or the associated controller will shut down.

4. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.

1	DCPM module orange locking button

5. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.

> The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

The DCPM module LED lights when the module is fully seated into the chassis.

Dispose of batteries

You must dispose of batteries according to the local regulations regarding battery recycling or disposal. If you cannot properly dispose of batteries, you must return the batteries to NetApp, as described in the RMA instructions that are shipped with the kit.

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the

replacement procedure.

Replace a DIMM - AFF A700 and FAS9000

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller

module.

1	Controller module cover locking button

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

1	DIMM ejector tabs
2	DIMM

4. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

5. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
7. Close the controller module cover.

Step 4: Install the controller

After you install the components into the controller module, you must install the controller module back into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
   e. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.

b. After the node boots to Maintenance mode, halt the node: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

- A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy node remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: *SLDIAG: No log messages are present.* a. Exit Maintenance mode: `halt` The node displays the LOADER prompt. b. Boot the node from the LOADER prompt: `bye` c. Return the node to normal operation.
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.

If the system-level diagnostics tests…	Then…
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a fan - AFF A700 and FAS9000

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

   > The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

1	Orange release button

5. Set the fan module aside.
6. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

   When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

7. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
8. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an I/O module - AFF A700 and FAS9000

To replace an I/O module, you must perform a specific sequence of tasks.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data

from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message`

`MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace I/O modules

To replace an I/O module, locate it within the chassis and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug any cabling associated with the target I/O module.

   Make sure that you label the cables so that you know where they came from.

3. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

4. Set the I/O module aside.
5. Install the replacement I/O module into the chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.
6. Recable the I/O module, as needed.

Step 3: Reboot the controller after PCIe module replacement

After you replace a PCIe module, you must reboot the controller module.

Steps

1. If the node is at the LOADER prompt, boot the node, responding `y` if you see a prompt warning of a system ID mismatch and asking to override the system ID: `bye`
2. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the `nicadmin convert` command from Maintenance mode.

   Be sure to exit Maintenance mode after completing the conversion.

3. Return the node to normal operation:

If your system is in…	Issue this command from the partner's console…
An HA pair	`storage failover giveback -ofnode` *`impaired_node_name`*
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.

4. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an LED USB module - AFF A700 and FAS9000

You can replace an LED USB module without interrupting service.

The FAS9000 or AFF A700 LED USB module provides connectivity to console ports and system status. Replacement of this module does not require tools.

Steps

1. Remove the old LED USB module:

a. With the bezel removed, locate the LED USB module at the front of the chassis, on the bottom left side.
b. Slide the latch to partially eject the module.
c. Pull the module out of the bay to disconnect it from the midplane. Do not leave the slot empty.

2. Install the new LED USB module:

a. Align the module to the bay with the notch in the corner of the module positioned near the slider latch on the chassis. The bay will prevent you from installing the module upside down.
b. Push the module into the bay until it is fully seated flush with the chassis.

   There is an audible click when the module is secure and connected to the midplane.

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVRAM module or NVRAM DIMMs - AFF A700 and FAS9000

The NVRAM module consists of the NVRAM10 and DIMMs and up to two NVMe SSD Flash Cache modules (FlashCache or caching modules) per NVRAM module. You can replace a failed NVRAM module or the DIMMs inside the NVRAM module. To replace a failed NVRAM module, you must remove it from the chassis, remove the FlashCache module or modules from the NVRAM module, move the DIMMs to the replacement module, reinstall the FlashCache module or modules, and install the replacement NVRAM module into the chassis. Because the system ID is derived from the NVRAM module, if replacing the module, disks belonging to the system are reassigned to the new system ID.

Before you begin

- All disk shelves must be working properly.
- If your system is in an HA pair, the partner node must be able to take over the node associated with the NVRAM module that is being replaced.
- This procedure uses the following terminology:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy* node is the HA partner of the impaired node.
- This procedure includes steps for automatically or manually reassigning disks to the controller module associated with the new NVRAM module. You must reassign the disks when directed to in the procedure. Completing the disk reassignment before giveback can cause issues.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You cannot change any disks or disk shelves as part of this procedure.

Step 1: Shut down the impaired controller

```
Shut down or take over the impaired controller using one of the following
options.
```

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a Two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace the NVRAM module

To replace the NVRAM module, locate it in slot 6 in the chassis and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Move the FlashCache module from the old NVRAM module to the new NVRAM module:

1	Orange release button (gray on empty FlashCache modules)
2	FlashCache cam handle

a. Press the orange button on the front of the FlashCache module.

> The release button on empty FlashCache modules is gray.

b. Swing the cam handle out until the module begins to slide out of the old NVRAM module.

c. Grasp the module cam handle and slide it out of the NVRAM module and insert it into the front of the new NVRAM module.

d. Gently push the FlashCache module all the way into the NVRAM module, and then swing the cam handle closed until it locks the module in place.

3. Remove the target NVRAM module from the chassis:

a. Depress the lettered and numbered cam button.

The cam button moves away from the chassis.

b. Rotate the cam latch down until it is in a horizontal position.

The NVRAM module disengages from the chassis and moves out a few inches.

c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

1	Lettered and numbered I/O cam latch
2	I/O latch completely unlocked

4. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.

1	Cover locking button
2	DIMM and DIMM ejector tabs

5. Remove the DIMMs, one at a time, from the old NVRAM module and install them in the replacement NVRAM module.
6. Close the cover on the module.
7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

Step 3: Replace a NVRAM DIMM

To replace NVRAM DIMMs in the NVRAM module, you must remove the NVRAM module, open the module, and then replace the target DIMM.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The NVRAM module disengages from the chassis and moves out a few inches.

c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

1	Lettered and numbered I/O cam latch
2	I/O latch completely unlocked

3. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.

1	Cover locking button
2	DIMM and DIMM ejector tabs

4. Locate the DIMM to be replaced inside the NVRAM module, and then remove it by pressing down on the DIMM locking tabs and lifting the DIMM out of the socket.

   Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.
6. Close the cover on the module.
7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

Step 4: Reboot the controller after FRU replacement

After you replace the FRU, you must reboot the controller module.

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Reassign disks

Depending on whether you have an HA pair or two-node MetroCluster configuration, you must either verify the reassignment of disks to the new controller module or manually reassign the disks.

Select one of the following options for instructions on how to reassign disks to the new controller.

Option 1: Verify ID (HA pair)

Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* node and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

Steps

1. If the replacement node is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the replacement node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.

   `boot_ontap bye`

   The node will reboot, if autoboot is set.

3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired node, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                      Takeover
Node              Partner             Possible     State Description
------------      ------------        --------
-------------------------------------
node1             node2               false        System ID changed
on partner (Old:
                                                    151759755, New:
151759706), In takeover
node2             node1               -            Waiting for
giveback (HA mailboxes)
```

4. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system`

```
node run -node local-node-name partner savecore -s
```

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

   a. From the healthy node, give back the replaced node's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* node takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration Guide for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the `System ID changed on partner` message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* node should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home
ID Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the node: `metrocluster node show`

   The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each node will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the node is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a node on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* node is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each node is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each node: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Option 2: Reassign ID (MetroCluster config)

Reassign the system ID in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering

`Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid`,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

```
dr-group-id cluster         node                 node-systemid dr-
partner-systemid
 ----------- --------------------- --------------------
------------- -------------------
 1           Cluster_A             Node_A_1             536872914
118073209
 1           Cluster_B             Node_B_1             118073209
536872914
 2 entries were displayed.
```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

```
Local System ID: 118065481
    ...
    ...
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                  POOL   SERIAL NUMBER  HOME
-------    -------------          -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Verify that the coredumps are saved: `system node run -node` *`local-node-name`* `partner savecore`

      If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node` *`local-node-name`* `partner savecore -s command`.</info>.

   c. Return to the admin privilege level: `set -privilege admin`
7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

       You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).
    b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`
    c. Return to the admin privilege level: `set -privilege admin`

Step 6: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key

management:

- Restore onboard key management encryption keys
- Restore external key management encryption keys

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A700 and FAS9000

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

> Do not mix PSUs with different efficiency ratings. Always replace like for like.

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.

> When removing a power supply, always use two hands to support its weight.

1	Locking button

5. Make sure that the on/off switch of the new power supply is in the Off position.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

   The power supplies are keyed and can only be installed one way.

   > Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Reconnect the power supply cabling:

   a. Reconnect the power cable to the power supply and the power source.

   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

8. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

   The green power LED lights when the PSU is fully inserted into the chassis and the amber attention LED flashes initially, but turns off after a few moments.

9. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization

continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

1	Controller module cover locking button

Step 3: Replace the RTC battery

To replace the RTC battery, you must locate the failed battery in the controller module, remove it from the holder, and then install the replacement battery in the holder.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

1	RTC battery
2	RTC battery housing

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
8. Reinstall the controller module cover.

Step 4: Reinstall the controller module and set time/date

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

Steps

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy node with the `show date` command.
   b. At the LOADER prompt on the target node, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target node.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the node reboot.
8. Return the node to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

X91148A module

Overview of adding an X91148A module - AFF A9000

You can add an I/O module to your system by either replacing a NIC or storage adapter with a new one in a fully-populated system, or by adding a new NIC or storage adapter into an empty chassis slot in your system.

Before you begin

- Check the NetApp Hardware Universe to make sure that the new I/O module is compatible with your system and version of ONTAP you're running.
- If multiple slots are available, check the slot priorities in NetApp Hardware Universe and use the best one available for your I/O module.
- To non-disruptively add an I/O module, you must takeover the target controller, remove the slot blanking cover in the target slot or remove an existing I/O module, add the new or replacement I/O module, and then giveback the target controller.
- Make sure that all other components are functioning properly.

Add an X91148A module in an AFF A700 with open slots - AFF A700 and FAS9000

You can add an X91148A module into an empty module slot in your system as either a 100GbE NIC or a storage module for the NS224 storage shelves.

- Your system must be running ONTAP 9.8 and later.
- To non-disruptively add the X91148A module, you must takeover the target controller, remove the slot blanking cover in the target slot, add the module, and then giveback the target controller.
- There must be one or more open slots available on your system.
- If multiple slots are available, install the module according to the slot priority matrix for the X91148A module in the Hardware Universe.

  NetApp Hardware Universe

- If you are adding the X91148A module as a storage module, you must install the module slots 3 and/or 7.
- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` command. See the Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

- All other components in the system must be functioning properly; if not, you must contact technical support.

Option 1: Add an X91148A module as a NIC module in a system with open slots

To add an X91148A module as a NIC module in a system with open slots, you must follow the specific sequence of steps.

Steps

1. Shutdown controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode` *`target_node_name`*

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.
2. If you are not already grounded, properly ground yourself.
3. Remove the target slot blanking cover:
   a. Depress the lettered and numbered cam button.
   b. Rotate the cam latch down until it is in a horizontal position.
   c. Remove the blanking cover.
4. Install the X91148A module:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
5. Cable the module to the data switches.
6. Reboot controller A: `boot_ontap`
7. Giveback the node from the partner node: `storage failover giveback -ofnode` *`target_node_name`*
8. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
9. Repeat these steps for controller B.

Option 2: Add an X91148A module as a storage module in a system with open slots

To add an X91148A module as a storage module in a system with open slots, you must follow the specific sequence of steps.

- This procedure presumes slots 3 and/or 7 are open.

Steps

1. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

2. If you are not already grounded, properly ground yourself.
3. Remove the target slot blanking cover:
   a. Depress the lettered and numbered cam button.
   b. Rotate the cam latch down until it is in a horizontal position.
   c. Remove the blanking cover.
4. Install the X91148A module into slot 3:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
   d. If you are installing a second X91148A module for storage, repeat this step for the module in slot 7.
5. Reboot controller A: `boot_ontap`
6. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`
7. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
8. Repeat these steps for controller B.
9. Install and cable your NS224 shelves, as described in Hot-add - NS224 shelves.

Add an X91148A storage module in a system with no open slots - AFF A700 and FAS9000

You must remove one more or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- Your system must be running ONTAP 9.8 and later.
- To non-disruptively add the X91148A module, you must takeover the target controller, add the module, and then giveback the target controller.
- If you are adding the X91148A module as a storage adapter, you must install the module in slots 3 and/or 7.
- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` command for each port. See the Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

- All other components in the system must be functioning properly; if not, you must contact technical support.

Option 1: Add an X91148A module as a NIC module in a system with no open slots

You must remove one or more existing NIC or storage modules in your system in order to

install one or more X91148A NIC modules into your fully-populated system.

Steps

1. If you are adding an X91148A module into a slot that contains a NIC module with the same number of ports as the X91148A module, the LIFs will automatically migrate when its controller module is shut down. If the NIC module being replaced has more ports than the X91148A module, you must permanently reassign the affected LIFs to a different home port. See Migrating a LIF for information about using System Manager to permanently move the LIFs
2. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode` *`target_node_name`*

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.
3. If you are not already grounded, properly ground yourself.
4. Unplug any cabling on the target I/O module.
5. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.
   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

6. Install the X91148A module into the target slot:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
7. Repeat the remove and install steps to replace additional modules for controller A.
8. Cable the module or modules to the data switches.
9. Reboot controller A: `boot_ontap`
10. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`
11. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
12. If you added the X91148A module as a NIC module in slots 3 or 7, for networking, use the `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` command for each port.
13. Repeat these steps for controller B.

Option 2: Adding an X91148A module as a storage module in a system with no open slots

You must remove one or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- This procedure presumes you re installing the X91148A module into slots 3 and/or 7.

Steps

1. If you are adding an X91148A module as a storage module in slots 3 and/or 7 into a slot that has an existing NIC module in it, use System Manager to permanently migrate the LIFs to different home ports, as described in Migrating a LIF.
2. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.
3. If you are not already grounded, properly ground yourself.
4. Unplug any cabling on the target I/O module.
5. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.
   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

6. Install the X91148A module into slot 3:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
   d. If you are installing a second X91148A module for storage, repeat the remove and install steps for the module in slot 7.
7. Reboot controller A: `boot_ontap`
8. Giveback the node from the partner node: `storage failover giveback -ofnode` *`target_node_name`*
9. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
10. Repeat these steps for controller B.
11. Install and cable your NS224 shelves, as described in Hot-adding an NS224 drive shelf.

AFF A700s System Documentation

Install and setup

Cluster configuration worksheet - AFF A700s

You can use the worksheet to gather and record your site-specific IP addresses and other information required when configuring an ONTAP cluster.

Cluster Configuration Worksheet

Start here: Choose your installation and setup experience

You can choose from different content formats to guide you through installing and setting up your new storage system.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

Installation and setup PDF poster - AFF A700s

You can use the PDF poster to install and set up your new system. The PDF poster provides step-by-step instructions with live links to additional content.

AFF A700s Installation and Setup Instructions

Installation and setup video - AFF A700s

The following video shows end-to-end software configuration for systems running ONTAP 9.2.

AFF A700s Setup Video

Maintain

Boot media

Overview of boot media replacement - AFF A700s

The primary boot media stores the ONTAP boot image that the system uses when it boots. You can restore the primary boot media image by using the ONTAP image on the secondary boot media, or if necessary, by using a USB flash drive.

If your secondary boot media has failed or is missing the image.tgz file, you must restore the primary boot media using a USB flash drive. The drive must be formatted to FAT32 and must have the appropriate amount of storage to hold the image_xxx.tgz file.

- The replacement process restores the var file system from the secondary boot media or USB flash drive to

the primary boot media.

- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

Check onboard encryption keys - AFF A700s

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If

so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes` manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

- Return to admin mode: `set -priv admin`
- Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

   - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   - Enter the command to display the OKM backup information: `security key-manager backup show`
   - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   - Return to admin mode: `set -priv admin`
   - Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

   - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

     > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

   - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
   - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   - Enter the command to back up the OKM information: `security key-manager backup show`

     > Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

   - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
   - Return to admin mode: `set -priv admin`
   - You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`

   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the

impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. Shut down the impaired controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. Shut down the impaired controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager external sync`

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. You can safely shut down the controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

Shut down the controller - AFF A700s

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller displays…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Replace the boot media - AFF A700s

You must remove the controller module from the chassis, open it, and then replace the failed boot media.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

1. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

2. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Risers
3	Air duct

Step 2: Replace the boot media - AFF A700s

You must locate the failed boot media in the controller module by removing the middle PCIe module on the controller module, locate the failed boot media by the lit LED near the boot media, and then replace the boot media.

You need a Phillips head screwdriver to remove the screw that holds the boot media in place.

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media:
   a. Open the air duct, if needed.
   b. If needed, remove Riser 2, the middle PCIe module, by unlocking the locking latch and then removing the riser from the controller module.

1	Air duct
2	Riser 2 (middle PCIe module)
3	Boot media screw
4	Boot media

3. Locate the failed boot media by the lit LED on the controller module motherboard.
4. Remove the boot media from the controller module:
   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
5. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
6. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

7. Rotate the boot media down until it is flush with the motherboard.
8. Secure the boot media in place by using the screw.

> Do not over-tighten the screw. Doing so might crack the boot media circuit board.

9. Reinstall the riser into the controller module.
10. Close the air duct:
    a. Rotate the air duct downward.
    b. Slide the air duct toward the risers until it clicks into place.

Transfer the boot image to the boot media - AFF A700s

You can install the system image to the replacement boot media using by using either the image on second boot media installed in the controller module, the primary method to restore the system image, or by transferring the boot image to the boot media using a USB flash drive when the secondary boot media restore failed or if the image.tgz file is not found on the secondary boot media.

Option 1: Transfer files to the boot media using backup recovery from the second boot media

You can install the system image to the replacement boot media using the image on second boot media installed in the controller module. This is the primary method for transferring the boot media files to the replacement boot media in systems with two boot media in the controller module.

The image on the secondary boot media must contain an `image.tgz` file and must not be reporting failures. If image.tgz file is missing or the boot media reports failures, you cannot use this procedure. You must transfer the boot image to the replacement boot media using the USB flash drive replacement procedure.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
    a. Swing the air duct all the way down to the controller module.
    b. Slide the air duct toward the risers until the locking tabs click into place.
    c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Air duct
2	Risers

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
4. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

5. Recable the power supply, and then connect it to the power source.

   Make sure that you reattach the power cable locking collar on the power cord.

6. Gently push the controller module all the way into the system until the controller module locking hooks begin to rise, firmly push on the locking hooks to finish seating the controller module, and then swing the locking hooks into the locked position over the pins on the controller module.

   The controller begins to boot as soon as it is completely installed into the chassis.

7. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

8. From the LOADER prompt, boot the recovery image from the secondary boot media: `boot_recovery`

   The image is downloaded from the secondary boot media.

9. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
10. After the image is installed, start the restoration process:
    a. Record the IP address of the impaired controller that is displayed on the screen.
    b. Press `y` when prompted to restore the backup configuration.
    c. Press `y` when prompted to confirm that the backup procedure was successful.
11. From the partner controller in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address` *`impaired_node_IP_address`*
12. After the configuration synchronization is complete without errors, press `y` when prompted to confirm that the backup procedure was successful.
13. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.
14. Exit advanced privilege level on the healthy controller.

Option 2: Transfer the boot image to the boot media using a USB flash drive

This procedure should only be used if the secondary boot media restore failed or if the image.tgz file is not found on the secondary boot media.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
    a. Swing the air duct all the way down to the controller module.
    b. Slide the air duct toward the risers until the locking tabs click into place.
    c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Air duct
2	Risers

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
4. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

5. Recable the power supply, and then connect it to the power source.

   Make sure that you reattach the power cable locking collar on the power cord.

6. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

7. Gently push the controller module all the way into the system until the controller module locking hooks begin to rise, firmly push on the locking hooks to finish seating the controller module, and then swing the locking hooks into the locked position over the pins on the controller module.

   The controller begins to boot as soon as it is completely installed into the chassis.

8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

9. Although the environment variables and bootargs are retained, you should check that all required boot environment variables and bootargs are properly set for your system type and configuration using the `printenv bootarg name` command and correct any errors using the `setenv variable-name <value>` command.
   a. Check the boot environment variables:
      - `bootarg.init.boot_clustered`
      - `partner-sysid`
      - `bootarg.init.flash_optimized` for AFF C190/AFF A220 (All Flash FAS)
      - `bootarg.init.san_optimized` for AFF A220 and All SAN Array
      - `bootarg.init.switchless_cluster.enable`
   b. If External Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:
      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `kmip.init.interface <value>`
      - `kmip.init.ipaddr <value>`
      - `kmip.init.netmask <value>`
      - `kmip.init.gateway <value>`
   c. If Onboard Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:
      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `bootarg.onboard_keymanager <value>`
   d. Save the environment variables you changed with the `savenv` command
   e. Confirm your changes using the `printenv` *`variable-name`* command.
10. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

    The image is downloaded from the USB flash drive.
11. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
12. After the image is installed, start the restoration process:
    a. Record the IP address of the impaired controller that is displayed on the screen.
    b. Press `y` when prompted to restore the backup configuration.
    c. Press `y` when prompted to confirm that the backup procedure was successful.
13. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.
14. From the partner controller in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address` *`impaired_node_IP_address`*

15. After the configuration synchronization is complete without errors, press `y` when prompted to confirm that the backup procedure was successful.
16. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.
17. Verify that the environmental variables are set as expected.
    a. Take the controller to the LOADER prompt.

       From the ONTAP prompt, you can issue the command 'system node halt -skip-lif-migration-before -shutdown true -ignore-quorum-warnings true -inhibit-takeover true'.

    b. Check the environment variable settings with the `printenv` command.
    c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
    d. Save your changes using the `savenv` command.
    e. Reboot the controller.
18. With the rebooted impaired controller displaying the `Waiting for giveback…` message, perform a giveback from the healthy controller:

If your system is in…	Then…
An HA pair	After the impaired controller is displaying the `Waiting for giveback…` message, perform a giveback from the healthy controller: a. From the healthy controller: `storage failover giveback -ofnode partner_node_name` The impaired controller takes back its storage, finishes booting, and then reboots and is again taken over by the healthy controller. ⓘ If the giveback is vetoed, you can consider overriding the vetoes. ONTAP 9 High-Availability Configuration Guide b. Monitor the progress of the giveback operation by using the `storage failover show-giveback` command. c. After the giveback operation is complete, confirm that the HA pair is healthy and that takeover is possible by using the `storage failover show` command. d. Restore automatic giveback if you disabled it using the `storage failover modify` command.

19. Exit advanced privilege level on the healthy controller.

Boot the recovery image - AFF A700s

You must boot the ONTAP image from the USB drive, restore the file system, and verify

the environmental variables.

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - AFF A700s

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


   ```
   ---------------------------BEGIN BACKUP---------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   ---------------------------END BACKUP---------------------------
   ```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int`

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A700s

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A700s

To replace the chassis, you must move the controller modules and SSD drives from the impaired chassis to the replacement chassis, and then remove the impaired chassis from the equipment rack or system cabinet and install the replacement chassis in its place.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the SSDs and controller modules to the new chassis, and that the replacement chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A700s

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Replace hardware - AFF A700s

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It click when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controllers

After you install the controller module into the new chassis, boot it to a state where you can run the diagnostic

test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. 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. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. 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.
6. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - AFF A700s

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:

a. Set the HA state for the chassis: `ha-config modify chassis HA-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `non-ha`

b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - AFF A700s

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- The healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- 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 A700s

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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the ontroller module hardware - AFF A700s

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properlcontrolleround yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Risers
3	Air duct

Step 2: Move the NVRAM card

As part of the controller replacement process, you must remove the NVRAM card from Riser 1 in the impaired controller module and install the card into Riser 1 of the replacement controller module. You should only reinstall Riser 1 into the replacement controller module after you have moved the DIMMs from the impaired controller module to the replacement controller module.

1. Remove the NVRAM riser, Riser 1, from the controller module:
   a. Rotate the riser locking latch on the left side of the riser up and toward the fans.

      The NVRAM riser raises up slightly from the controller module.

   b. Lift the NVRAM riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser straight up out of the controller module, and then place it on a stable, flat surface so that you can access the NVRAM card.

1	Air duct
2	Riser 1 locking latch
3	NVRAM battery cable plug connecting to the NVRAM card
4	Card locking bracket
5	NVRAM card

2. Remove the NVRAM card from the riser module:
   a. Turn the riser module so that you can access the NVRAM card.
   b. Unplug the NVRAM battery cable that is attached to the NVRAM card.
   c. Press the locking bracket on the side of the NVRAM riser, and then rotate it to the open position.
   d. Remove the NVRAM card from the riser module.
3. Remove the NVRAM riser from the replacement controller module.
4. Install the NVRAM card into the NVRAM riser:
   a. Align the card with the card guide on the riser module and the card socket in the riser.
   b. Slide the card squarely into the card socket.

> Make sure that the card is completely and squarely seated into the riser socket.

c. Connect the battery cable to the socket on the NVRAM card.

d. Swing the locking latch into the locked position and make sure that it locks in place.

Step 3: Move PCIe cards

As part of the controller replacement process, you must remove both PCIe riser modules, Riser 2 (the middle riser) and Riser 3 (riser on the far right) from the impaired controller module, remove the PCIe cards from the riser modules, and install them in the same riser modules in the replacement controller module. You will install the riser modules into the replacement controller module once the DIMMs have been moved to the replacement controller module.

1. Remove the PCIe riser from the controller module:

   a. Remove any SFP modules that might be in the PCIe cards.

   b. Rotate the module locking latch on the left side of the riser up and toward the fan modules.

      The PCIe riser raises up slightly from the controller module.

   c. Lift the PCIe riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.

1	Air duct
2	Riser locking latch
3	Card locking bracket

4	Riser 2 (middle riser) and PCI cards in riser slots 2 and 3.

2. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. Remove the PCIe card from the riser.
3. Remove the corresponding riser from the replacement controller module.
4. Install the PCIe card into the same slot in PCIe riser:
   a. Align the card with the card guide on the riser and the card socket in the riser, and then slide it squarely into the socket in the riser.

      Make sure that the card is completely and squarely seated into the riser socket.

   b. Swing the locking latch into place until it clicks into the locked position.
5. Repeat the preceding steps for Riser 3 and PCIe cards in slots 4 and 5 in the impaired controller module.

Step 4: Move the boot media

There are two boot media devices in the AFF A700s, a primary and a secondary or backup boot media. You must move them from the impaired controller to the *replacement* controller and install them into their respective slots in the *replacement* controller.

The boot media are located under Riser 2, the middle PCIe riser module. This PCIe module must be removed to gain access to the boot media.

1. Locate the boot media:
   a. Open the air duct, if needed.
   b. If needed, remove Riser 2, the middle PCIe module, by unlocking the locking latch and then removing the riser from the controller module.

+

1	Air duct
2	Riser 2 (middle PCIe module)
3	Boot media screw
4	Boot media

2. Remove the boot media from the controller module:
   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
3. Move the boot media to the new controller module and install it:

> Install the boot media into the same socket in the replacement controller module as it was installed in the impaired controller module; primary boot media socket (slot 1) to primary boot media socket, and secondary boot media socket (slot 2) to secondary boot media socket.

   a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.

b. Rotate the boot media down toward the motherboard.

c. Secure the boot media to the motherboard using the boot media screw.

   Do not over-tighten the screw or you might damage the boot media.

Step 5: Move the fans

You must move the fans from the impaired controller module to the replacement module when replacing a failed controller module.

1. Remove the fan module by pinching the locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan locking tabs
2	Fan module

2. Move the fan module to the replacement controller module, and then install the fan module by aligning its edges with the opening in the controller module, and then sliding the fan module into the controller module until the locking latches click into place.
3. Repeat these steps for the remaining fan modules.

Step 6: Move system DIMMs

To move the DIMMs, locate and move them from the impaired controller into the replacement controller and follow the specific sequence of steps.

1. Locate the DIMMs on your controller module.

1	Air duct
2	Riser 1 and DIMM bank 1-4
3	Riser 2 and DIMM banks 5-8 and 9-12
4	Riser 3 and DIMM bank 13-16

2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

   Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

4. Locate the slot where you are installing the DIMM.
5. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. 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. Repeat these steps for the remaining DIMMs.

Step 7: Install the NVRAM module

To install the NVRAM module, you must follow the specific sequence of steps.

1. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP modules that were removed from the PCIe cards.

Step 8: Move the NVRAM battery

When replacing the controller module, you must move the NVRAM battery from the impaired controller module to the replacement controller module

1. Locate the NVRAM battery on the left side of the riser module, Riser 1.

1	NVRAM battery plug
2	Blue NVRAM battery locking tab

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Move the battery pack to the replacement controller module, and then install it in the NVRAM riser:
   a. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook

into the slots on the battery pack, and the battery pack latch engages and locks into place.

b. Press firmly down on the battery pack to make sure that it is locked into place.

c. Plug the battery plug into the riser socket and make sure that the plug locks into place.

Step 9: Install a PCIe riser

To install a PCIe riser, you must follow a specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP modules that were removed from the PCIe cards.
3. Repeat the preceding steps for Riser 3 and PCIe cards in slots 4 and 5 in the impaired controller module.

Step 10: Move the power supply

You must move the power supply and power supply blank from the impaired controller module to the replacement controller module when you replace a controller module.

1. If you are not already grounded, properly ground yourself.
2. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab

❷	Power supply

3. Move the power supply to the new controller module, and then install it.
4. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

5. Remove the PSU blanking panel from the impaired controller module, and then install it in the replacement controller module.

Step 11: Install the controller module

After all the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis and then boot it to Maintenance mode.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

+

1	Locking tabs
2	Slide plunger

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. 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.
7. 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.

Restore and verify the system configuration - AFF A700s

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the chassis

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - ha
   - non-ha

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

Recable the system and reassign disks - AFF A700s

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: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                    Takeover
Node              Partner           Possible     State Description
------------      ------------      --------
-------------------------------------
node1             node2             false        System ID changed on
partner (Old:
                                                 151759755, New:
151759706), In takeover
node2             node1             -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node` *`local-node-name`* `partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover`

`giveback -ofnode replacement_node_name`

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

   The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

Complete system restoration - AFF A700s

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement node in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement*

node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A700s

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Shut down the impaired controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller.

ONTAP 9 System Administration Reference

Steps

1. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
2. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y`.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows `Waiting for giveback…`, press Ctrl-C, and then respond `y`.

Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

❶	Locking latch
❷	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

❶	Air duct locking tabs
❷	Risers
❸	Air duct

Replace a DIMM

To replace a DIMM, you must locate it in the controller module using the DIMM map on the inside of the controller module or locating it using the LED next to the DIMM, and then replace it following the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.

2. Remove the applicable riser.

1	Air duct cover
2	Riser 1 and DIMM bank 1-4
3	Riser 2 and DIMM bank 5-8 and 9-12
4	Riser 3 and DIMM 13-16

   - If you are removing or moving a DIMM in bank 1-4, unplug the NVRAM battery, unlock the locking latch on Riser 1, and then remove the riser.
   - If you are removing or moving a DIMM in bank 5-8 or 9-12, unlock the locking latch on Riser 2, and then remove the riser.
   - If you are removing or moving a DIMM in bank 13-16, unlock the locking latch on Riser 3, and then remove the riser.
3. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
4. Eject the DIMM from its 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.

5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
8. Reinstall any risers that you removed from the controller module.

   If you removed the NVRAM riser, Riser 1, make sure that you plug the NVRAM battery into the controller module.

9. Close the air duct.

Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

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. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. 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.

Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF A700s

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.

- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Fan

Shut down the impaired controller - AFF A700s

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Remove the controller module - AFF A700s

You must remove the controller module from the chassis when you replace the controller

module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.

b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Risers
3	Air duct

Replacing a fan - AFF A700s

To replace a fan, remove the failed fan module and replace it with a new fan module.

1. If you are not already grounded, properly ground yourself.
2. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
3. Remove the fan module by pinching the locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan locking tabs
2	Fan module

4. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module until the locking latches click into place.

Reinstall the controller module - AFF A700s

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Locking tabs
2	Slide plunger

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

7. 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.

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`

Return the failed part to NetApp - AFF A700s

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVRAM battery - AFF A700s

To replace an NVRAM battery in the system, you must remove the controller module from the system, remove the battery, replace the battery, and then reinstall the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Shut down the impaired controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Set the controller module aside in a safe place.

Replace the NVRAM battery

To replace the NVRAM battery, you must remove the failed NVRAM battery from the controller module and install the replacement NVRAM battery into the controller module.

1. If you are not already grounded, properly ground yourself.
2. Locate the NVRAM battery on the left side of the riser module, Riser 1.

1	NVRAM battery plug
2	Blue NVRAM battery locking tab

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Push the blue locking tab on the battery holder, so that the latch releases from the holder.
5. Slide the battery down the riser bracket, lift the battery out of the controller, and then set it aside.
6. Slide the replacement battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and locks into place.
7. Plug the battery plug into the riser socket and make sure that the plug locks into place.

Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Locking tabs
2	Slide plunger

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

7. 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.

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`

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVRAM module and NVRAM DIMMs - AFF A700s

To replace a failed NVRAM card, you must remove the NVRAM riser, Riser 1, from the controller module, remove the failed card from the riser, install the new NVRAM card in the riser, and then reinstall the riser in the controller module. Because the system ID is derived from the NVRAM card, if replacing the module, disks belonging to the system are reassigned to the new system ID.

Before you begin

- All disk shelves must be working properly.
- If your system is in an HA pair, the partner 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.

Shut down the impaired controller

Steps

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

   - 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

Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Risers
3	Air duct

Remove the NVRAM card

Replacing the NVRAM consist of removing the NVRAM riser, Riser 1, from the controller module, disconnecting the NVRAM battery from the NVRAM card, removing the failed NVRAM card and installing the replacement NVRAM card, and then reinstalling the NVRAM riser back into the controller module.

1. If you are not already grounded, properly ground yourself.
2. Remove the NVRAM riser, Riser 1, from the controller module:
   a. Rotate the riser locking latch on the left side of the riser up and toward the fans.

      The NVRAM riser raises up slightly from the controller module.

   b. Lift the NVRAM riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser straight up out of the controller module, and then place it on a stable, flat surface so that you can access the NVRAM card.

1	Air duct
2	Riser 1 locking latch
3	NVRAM battery cable plug connecting to the NVRAM card
4	Card locking bracket
5	NVRAM card

3. Remove the NVRAM card from the riser module:
   a. Turn the riser module so that you can access the NVRAM card.
   b. Unplug the NVRAM battery cable that is attached to the NVRAM card.
   c. Press the locking bracket on the side of the NVRAM riser, and then rotate it to the open position.
   d. Remove the NVRAM card from the riser module.
4. Install the NVRAM card into the NVRAM riser:
   a. Align the card with the card guide on the riser module and the card socket in the riser.
   b. Slide the card squarely into the card socket.

      Make sure that the card is completely and squarely seated into the riser socket.

   c. Connect the battery cable to the socket on the NVRAM card.

d. Swing the locking latch into the locked position and make sure that it locks in place.

5. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP modules that were removed from the PCIe cards.

Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

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. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. 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.

Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

   ```
   node1> `storage failover show`
                                       Takeover
   Node              Partner           Possible     State Description
   ------------      ------------      --------
   -------------------------------------
   node1             node2             false        System ID changed on
   partner (Old:
                                                     151759755, New:
   151759706), In takeover
   node2             node1             -            Waiting for giveback
   (HA mailboxes)
   ```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node` *`local-node-name`* `partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration Guide for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

   The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. Verify that the expected volumes are present for each controller: `vol show -node node-name`
8. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

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

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe card - AFF A700s

To replace a PCIe card, you must disconnect the cables from the cards in the riser, remove the riser, replace the riser, and then recable the cards in that riser.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

+

1	Air duct locking tabs
2	Risers
3	Air duct

Step 3: Replace a PCIe card

To replace a PCIe card, you must remove the cabling and any SFPs from the ports on the PCIe cards in the target riser, remove the riser from the controller module, remove and replace the PCIe card, reinstall the riser, and recable it.

1. If you are not already grounded, properly ground yourself.
2. Remove the PCIe riser from the controller module:
   a. Remove any SFP modules that might be in the PCIe cards.
   b. Rotate the module locking latch on the left side of the riser up and toward the fan modules.

      The PCIe riser raises up slightly from the controller module.

   c. Lift the PCIe riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.

1	Air duct
2	Riser locking latch
3	Card locking bracket
4	Riser 2 (middle riser) and PCI cards in riser slots 2 and 3.

3. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. Remove the PCIe card from the riser.
4. Install the PCIe card into the same slot in PCIe riser:
   a. Align the card with the card guide on the riser and the card socket in the riser, and then slide it squarely into the socket in the riser.

      Make sure that the card is completely and squarely seated into the riser socket.

   b. Swing the locking latch into place until it clicks into the locked position.
5. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller

module.

c. Swing the locking latch down and click it into the locked position.

   When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

d. Reinsert any SFP modules that were removed from the PCIe cards.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Locking tabs
2	Slide plunger

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
7. 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.

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

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A700s

Swapping out a power supply involved disconnecting the target power supply (PSU) from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting it to the power source.

- The power supplies are redundant and hot-swappable.

- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

Steps

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab
2	Power supply

5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Close the cam handle by swinging it down as far as it will go.
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. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A700s

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.

Shut down the impaired controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Risers
3	Air duct

Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

1	Air duct
2	RTC battery and housing

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
6. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

System-Level Diagnostics for AFF A700s

System-Level Diagnostics for AFF A700s is available outside this library. You will be prompted to log in using your NetApp Support Site credentials.

AFF A700s System-Level Diagnostics

AFF A800 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations (including ASA configurations), you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick steps - AFF A800

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use the AFF A800 Systems Installation and Setup Instructions if you are familiar with installing NetApp systems.

Videos - AFF A800

There are two videos - one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and Setup of an AFF A800

Video two of two: Perform end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed steps - AFF A800

This section gives detailed step-by-step instructions for installing an AFF A800 system.

Step 1: Prepare for installation

To install your AFF A800 system, you need to create an account and register the system. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the NetApp Hardware Universe (HWU) for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

What you need

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
  1. Unpack the contents of all boxes.
  2. Record the system serial number from the controllers.

Steps

1. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register (NetApp Product Registration) your system.
2. Download and install NetApp Downloads: Config Advisor on your laptop.
3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the NetApp Hardware Universe to locate the cable and identify its use.

Connector type	Part number and length	Type of cable…	For…
100 GbE cable	X66211A-05 (112-00595), 0.5m		HA interconnect
	X66211A-05 (112-00595), 0.5m; X66211-1 (112-00573), 1m		Cluster interconnect network
	X66211-2 (112-00574), 2m; X66211-5 (112-00576), 5m		Storage, Data
10 GbE cable	X6566B-3-R6 (112-00300), 3m; X6566B-5-R6 (112-00301), 5m		Data
25 GbE cable	X66240A-2 (112-00598), 2m; X66240A-5 (112-00600), 5m		Data
RJ-45 (order dependent)	Not applicable		Management
Fibre Channel	X66250-2 (112-00342) 2m; X66250-5 (112-00344) 5m; X66250-15 (112-00346) 15m; X66250-30 (112-00347) 30m		
Micro-USB console cable	Not applicable		Console connection during software setup
Power cables	Not applicable		Powering up the system

4. Download and complete the Cluster Configuration Worksheet.

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.

   Installing SuperRail into a four-post rack

2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.

3. Attach cable management devices (as shown).

4. Place the bezel on the front of the system.

Step 3: Cable controllers

There is required cabling for your platform's cluster using the two-node switchless cluster method or the cluster interconnect network method. There is optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cable to a host network and storage.

Required cabling: Cable controllers to a cluster

Cable the controllers to a cluster by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster

Management network ports on the controllers are connected to switches. The HA interconnect and cluster interconnect ports are cabled on both controllers.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cable a two-node switchless cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller module
1	Cable the HA interconnect ports: • e0b to e0b • e1b to e1b
2	Cable the cluster interconnect ports: • e0a to e0a • e1a to e1a

Step	Perform on each controller module
3	Cable the management ports to the management network switches
!	DO NOT plug in the power cords at this point.

2. To perform optional cabling, see:
   - [Option 1: Connect to a Fibre Channel host]
   - [Option 2: Connect to a 10GbE host]
   - [Option 3: Connect to a single direct-attached NS224 drive shelf]
   - [Option 4: Connect to two direct-attached NS224 drive shelves]
3. To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 2: Cable a switched cluster

Cluster interconnect and management network ports on the controllers are connected to switches while the HA interconnect ports are cabled on both controllers.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cabling a switched cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller module
1	Cable the HA interconnect ports: • e0b to e0b • e1b to e1b

Step	Perform on each controller module
2	Cable the cluster interconnect ports to the 100 GbE cluster interconnect switches. **e0a** e1a
3	Cable the management ports to the management network switches
!	DO NOT plug in the power cords at this point.

2. To perform optional cabling, see:
    - [Option 1: Connect to a Fibre Channel host]
    - [Option 2: Connect to a 10GbE host]
    - [Option 3: Connect to a single direct-attached NS224 drive shelf]
    - [Option 4: Connect to two direct-attached NS224 drive shelves]
3. To complete setting up your system, see Step 4: Complete system setup and configuration.

Optional cabling: Cable configuration-dependent options

You have configuration-dependent optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cabling to a host network and storage.

Option 1: Cable to a Fibre Channel host network

Fibre Channel ports on the controllers are connected to Fibre Channel host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Step	Perform on each controller module
1	Cable ports 2a through 2d to the FC host switches.
2	To perform other optional cabling, choose from: • [Option 3: Connect to a single direct-attached NS224 drive shelf] • [Option 4: Connect to two direct-attached NS224 drive shelves]
3	To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 2: Cable to a 10GbE host network

10GbE ports on the controllers are connected to 10GbE host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Step	Perform on each controller module
1	Cable ports e4a through e4d to the 10GbE host network switches.
2	To perform other optional cabling, choose from: • [Option 3: Connect to a single direct-attached NS224 drive shelf] • [Option 4: Connect to two direct-attached NS224 drive shelves]
3	To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 3: Cable the controllers to a single drive shelf

You must cable each controller to the NSM modules on the NS224 drive shelf.

Before you begin

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cabling the controllers to a single drive shelf or the step-by-step instructions to cable

your controller modules to a single shelf.

Step	Perform on each controller module
1	Cable controller A to the shelf:
2	Cable controller B to the shelf:

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 4: Cable the controllers to two drive shelves

You must cable each controller to the NSM modules on both NS224 drive shelves.

Before you begin

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation (Cabling the controllers to two drive shelves) or the written steps to cable your controllers to two drive shelves.

Step	Perform on each controller module
1	Cable controller A to the shelves:

Step	Perform on each controller module
2	Cable controller B to the shelves:

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Step 4: Complete system setup and configuration

Complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Complete system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   The system begins to boot. Initial booting may take up to eight minutes.

2. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

3. Use the following animation (Connecting your laptop to the Management switch) to connect your laptop to

the Management switch.

4. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click **Network** in the left pane.
   c. Right-click and select **refresh**.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

5. Use System Manager guided setup to configure your system using the data you collected in the ONTAP Configuration Guide.
6. Verify the health of your system by running Config Advisor.
7. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Complete system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

   > See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console, and connect the console port on the controller using the console cable that came with your system.

c. Connect the laptop or console to the switch on the management subnet.

d. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   The system begins to boot. Initial booting may take up to eight minutes.

3. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

4. Using System Manager on your laptop or console, configure your cluster:

a. Point your browser to the node management IP address.

> The format for the address is https://x.x.x.x.

b. Configure the system using the data you collected in the ONTAP Configuration Guide.

5. Verify the health of your system by running Config Advisor.
6. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A800

- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

Check onboard encryption keys - AFF A800

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to [Checking NVE or NSE on systems running ONTAP 9.5 and later].
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Checking NVE or NSE on systems running ONTAP 9.6 and later].
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`

   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.
   b. If the `Restored` column displays anything other than `yes`:
      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        > Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Restore the external key management authentication keys to all nodes in the cluster: `security`

`key-manager external restore`

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller. Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: System is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A800

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 2: Replace the boot media

You locate the failed boot media in the controller module by removing Riser 3 on the controller module before you can replace the boot media.

You need a Phillips head screwdriver to remove the screw that holds the boot media in place.

1. Locate the boot media:

1	Air duct
2	Riser 3
3	Phillips #1 screwdriver
4	Boot media screw
5	Boot media

2. Remove the boot media from the controller module:
   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
3. Install the replacement boot media into the controller module:
   a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.
   b. Rotate the boot media down toward the motherboard.
   c. Secure the boot media to the motherboard using the boot media screw.

      Do not over-tighten the screw or you might damage the boot media.
4. Reinstall the riser into the controller module.

5. Close the air duct:
   a. Rotate the air duct downward.
   b. Slide the air duct toward the risers until it clicks into place.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed is without a boot image so you need to transfer a boot image using a USB flash drive.

Before you begin

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
   a. Download the service image to your work space on your laptop.
   b. Unzip the service image.

      NOTE: If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

      There are two folders in the unzipped service image file:
      +
      - boot
      - efi
   c. Copy the efi folder to the top directory on the USB flash drive.

      The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.
   d. Remove the USB flash drive from your laptop.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Air duct
2	Risers

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
4. Reinstall the cable management device and recable the system, as needed.
   +
   When recabling, remember to reinstall the media converters (SFPs or QSFPs) if they were removed.
5. Plug the power cable into the power supply and reinstall the power cable retainer.
6. Insert the USB flash drive into the USB slot on the controller module.
   +
   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.
7. Gently push the controller module all the way into the system until the controller module locking hooks begin to rise, firmly push on the locking hooks to finish seating the controller module, and then swing the locking hooks into the locked position over the pins on the controller module.
   +
   The controller begins to boot as soon as it is completely installed into the chassis.
8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.
   +
   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

Boot the recovery image - AFF A800

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press **`y`**.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press **`y`**.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment_variable_name changed_value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - AFF A800

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.

3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int`

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A800

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Replace the chassis - AFF A800

To replace the chassis, you must move the bezel, controller modules, and NVMe drives from the impaired chassis to the replacement chassis, and then remove the impaired chassis from the equipment rack or system cabinet and install the replacement chassis in its place.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the bezel, NVMe drives, and controller modules to the new chassis, and that the replacement chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A800

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Move and replace hardware - AFF A800

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the

equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run the diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Interrupt the normal boot process by pressing `Ctrl-C`.
5. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - AFF A800

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

The value for HA-state can be one of the following:

- `ha`
- `mcc`
- `mccip`
- `non-ha`

b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - AFF A800

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.

- The healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller’s console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

> Do not downgrade the BIOS version of the *replacement* controller to match the partner controller or the old controller module.

Shut down the impaired controller - AFF A800

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the controller module hardware - AFF A800

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 2: Move the power supplies

You must move the power supplies from the impaired controller module to the replacement controller module when you replace a controller module.

1. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab
2	Power supply

2. Move the power supply to the new controller module, and then install it.
3. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

Step 3: Move the fans

You must move the fans from the impaired controller module to the replacement module when replacing a failed controller module.

1. Remove the fan module by pinching the locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan locking tabs
2	Fan module

2. Move the fan module to the replacement controller module, and then install the fan module by aligning its edges with the opening in the controller module, and then sliding the fan module into the controller module until the locking latches click into place.
3. Repeat these steps for the remaining fan modules.

Step 4: Move the NVDIMM battery

When replacing the controller module, you must move the NVRAM battery from the impaired controller module to the replacement controller module

1. Open the air duct cover and locate the NVDIMM battery in the riser.

1	Air duct riser
2	NVDIMM battery plug
3	NVDIMM battery pack

Attention: The NVDIMM battery control board LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
3. Grasp the battery and lift the battery out of the air duct and controller module.
4. Move the battery pack to the replacement controller module and then install it in the NVDIMM air duct:
   a. Insert the battery pack into the slot and press firmly down on the battery pack to make sure that it is locked into place.
   b. Plug the battery plug into the riser socket and make sure that the plug locks into place.

Step 5: Remove the PCIe risers

As part of the controller replacement process, you must remove the PCIe modules from the impaired controller module. You must install them into the same location in the replacement controller module once the NVDIMMS and DIMMs have moved to the replacement controller module.

1. Remove the PCIe riser from the controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward the fan modules.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.

1	Air duct
2	Riser 1 (left riser), Riser 2 (middle riser), and 3 (right riser) locking latches

2. Repeat the preceding step for the remaining risers in the impaired controller module.
3. Repeat the above steps with the empty risers in the replacement controller and put them away.

Step 6: Move system DIMMs

To move the DIMMs, locate and move them from the impaired controller into the replacement controller and follow the specific sequence of steps.

1. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.

2. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

3. Locate the slot where you are installing the DIMM.
4. Insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

> Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

5. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
6. Repeat these steps for the remaining DIMMs.

Step 7: Move the NVDIMMs

To move the NVDIMMs, locate and move them from the impaired controller into the replacement controller and follow the specific sequence of steps.

1. Locate the NVDIMMs on your controller module.

1	Air duct

❷	NVDIMMs

2. Note the orientation of the NVDIMM in the socket so that you can insert the NVDIMM in the replacement controller module in the proper orientation.
3. Eject the NVDIMM from its slot by slowly pushing apart the two NVDIMM ejector tabs on either side of the NVDIMM, and then slide the NVDIMM out of the socket and set it aside.

   ⓘ Carefully hold the NVDIMM by the edges to avoid pressure on the components on the NVDIMM circuit board.

4. Locate the slot where you are installing the NVDIMM.
5. Insert the NVDIMM squarely into the slot.

   The NVDIMM fits tightly in the slot, but should go in easily. If not, realign the NVDIMM with the slot and reinsert it.

   ⓘ Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
7. Repeat the preceding steps to move the other NVDIMM.

Step 8: Move the boot media

There is one boot media device in the AFF A800. You must move it from the impaired controller and install it in the *replacement* controller.

The boot media is located under Riser 3.

1. Locate the boot media:

1	Air duct
2	Riser 3
3	Phillips #1 screwdriver
4	Boot media screw
5	Boot media

2. Remove the boot media from the controller module:
   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
3. Move the boot media to the new controller module and install it:
   a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.
   b. Rotate the boot media down toward the motherboard.
   c. Secure the boot media to the motherboard using the boot media screw.

      Do not over-tighten the screw or you might damage the boot media.

Step 9: Install the PCIe risers

You install the PCIe risers in the replacement controller module after moving the DIMMs, NVDIMMs, and boot media.

1. Install the riser into the replacement controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP or QSFP modules that were removed from the PCIe cards.
2. Repeat the preceding step for the remaining PCIe risers.

Step 10: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis and then boot it to Maintenance mode.

1. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

❶	Locking tabs
❷	Slide plunger

2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   ⓘ Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   ⓘ You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. Interrupt the normal boot process by pressing `Ctrl-C`.
5. Plug the system cables and transceiver modules into the controller module and reinstall the cable management device.
6. Plug the power cables into the power supplies and reinstall the power cable retainers.

Restore and verify the system configuration - AFF A800

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the chassis

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mccip`
   - `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

Recable the system and reassign disks - AFF A800

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node` *`local-node-name`* `partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

   The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node show`

   The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* controller is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each controller is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each controller: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A800

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

> The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A800

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

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.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 3: Replace a DIMM

To replace a DIMM, you must locate it in the controller module using the DIMM map label on top of the air duct or locating it using the LED next to the DIMM, and then replace it following the specific sequence of steps.

1. When removing a DIMM, unlock the locking latch on the applicable riser, and then remove the riser.

1	Air duct cover
2	Riser 1 and DIMM bank 1, and 3-6
Riser 2 and DIMM bank 7-10, 12-13, and 15-18	Riser 3 and DIMM 19 -22 and 24

Note: Slot 2 and 14 are left empty. Do not attempt to install DIMMs into these slots.

2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

4. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

5. Insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
7. Reinstall any risers that you removed from the controller module.
8. Close the air duct.

Step 4: Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

1. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

❶	Locking tabs
❷	Slide plunger

2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   ⓘ Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
    - If the test failed, correct the failure, and then rerun the test.
    - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF A800

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive

and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a fan - AFF A800

To replace a fan, remove the failed fan module and replace it with a new fan module.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a fan module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables from the controller module, keeping track of where the cables were connected.

Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Set the controller module aside in a safe place.

Step 3: Replace a fan

To replace a fan, remove the failed fan module and replace it with a new fan module.

1. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
2. Remove the fan module by pinching the locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan locking tabs
2	Fan module

3. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module until the locking latches click into place.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the system, as needed.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

c. If you have not already done so, reinstall the cable management device.

5. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`

6. If automatic giveback was disabled, reenable it: `storage failover modify -controller local -auto-giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an NVDIMM - AFF A800

You must replace the NVDIMM in the controller module when your system registers that the flash lifetime is almost at an end or that the identified NVDIMM is not healthy in general; failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Place the controller module on a stable, flat surface, and then open the air duct:

   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

+

1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 3: Replace the NVDIMM

To replace the NVDIMM, you must locate it in the controller module using the NVDIMM map label on top of the air duct or locating it using the LED next to the NVDIMM, and then replace it following the specific sequence of steps.

The NVDIMM LEDs blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.

1. If you are removing or moving an NVDIMM, unlock the locking latch on the riser, and then remove the applicable riser.

1	Air duct cover
2	Riser 2 and NVDIMM 11

2. Note the orientation of the NVDIMM in the socket so that you can insert the NVDIMM in the replacement controller module in the proper orientation.
3. Eject the NVDIMM from its slot by slowly pushing apart the two NVDIMM ejector tabs on either side of the NVDIMM, and then slide the NVDIMM out of the socket and set it aside.

> Carefully hold the NVDIMM by the edges to avoid pressure on the components on the NVDIMM circuit board.

4. Remove the replacement NVDIMM from the antistatic shipping bag, hold the NVDIMM by the corners, and then align it to the slot.

   The notch among the pins on the NVDIMM should line up with the tab in the socket.

5. Locate the slot where you are installing the NVDIMM.
6. Insert the NVDIMM squarely into the slot.

   The NVDIMM fits tightly in the slot, but should go in easily. If not, realign the NVDIMM with the slot and reinsert it.

   > Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
8. Reinstall any risers that you removed from the controller module.
9. Close the air duct.

Step 4: Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

1. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Locking tabs
2	Slide plunger

2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

c. If you have not already done so, reinstall the cable management device.

d. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 4: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Select **NVDIMM Test** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVDIMM battery - AFF A800

To replace the NVDIMM battery, you must remove the controller module, remove the battery, replace the battery, and then reinstall the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Set the controller module aside in a safe place.

Step 3: Replace the NVDIMM battery

To replace the NVDIMM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module.

1. Open the air duct cover and locate the NVDIMM battery in the riser.

1	Air duct riser
2	NVDIMM battery plug
3	NVDIMM battery pack

Attention: The NVDIMM battery control board LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
3. Grasp the battery and lift the battery out of the air duct and controller module, and then set it aside.
4. Remove the replacement battery from its package.
5. Install the replacement battery pack in the NVDIMM air duct:
   a. Insert the battery pack into the slot and press firmly down on the battery pack to make sure that it is locked into place.

b. Plug the battery plug into the riser socket and make sure that the plug locks into place.

6. Close the NVDIMM air duct.

   Make sure that the plug locks into the socket.

Step 4: Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

3. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
4. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Interrupt the normal boot process by pressing `Ctrl-C`.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe card - AFF A800

To replace a PCIe card, you must disconnect the cables from the cards, remove the SFP and QSFP modules from the cards before removing the riser, reinstall the riser, and then reinstall the SFP and QSFP modules before cabling the cards.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

7. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 3: Replace a PCIe card

To replace a PCIe card, you must remove the cabling and any QSFPs and SFPs from the ports on the PCIe cards in the target riser, remove the riser from the controller module, remove and replace the PCIe card, reinstall the riser and any QSFPs and SFPs onto the ports, and cable the ports.

1. Determine if the card you are replacing is from Riser 1 or if it is from Riser 2 or 3.
   - If you are replacing the 100GbE PCIe card in Riser 1, use Steps 2 - 3 and Steps 6 - 7.

- If you are replacing a PCIe card from Riser 2 or 3, use Steps 4 through 7.

2. Remove Riser 1 from the controller module:
   a. Remove the QSFP modules that might be in the PCIe card.
   b. Rotate the riser locking latch on the left side of the riser up and toward the fan modules.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.

1	Air duct
2	Riser locking latch
3	Card locking bracket
4	Riser 1 (left riser) with 100GbE PCIe card in slot 1.

3. Remove the PCIe card from Riser 1:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. Remove the PCIe card from the riser.
4. Remove the PCIe riser from the controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward the fan modules.

The riser raises up slightly from the controller module.

c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.

1	Air duct
2	Riser 2 (middle riser) or 3 (right riser) locking latch
3	Card locking bracket
4	Side panel on riser 2 or 3
5	PCIe cards in riser 2 or 3

5. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe cards.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. Swing the side panel off the riser.
   d. Remove the PCIe card from the riser.
6. Install the PCIe card into the same slot in the riser:
   a. Align the card with the card socket in the riser, and then slide it squarely into the socket in the riser.

   > Make sure that the card is completely and squarely seated into the riser socket.

   b. For Riser 2 or 3, close the side panel.
   c. Swing the locking latch into place until it clicks into the locked position.
7. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.

b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.

c. Swing the locking latch down and click it into the locked position.

   When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

d. Reinsert any SFP modules that were removed from the PCIe cards.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.

1	Locking tabs
2	Slide plunger

2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.
4. Plug the power cables into the power supplies and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
6. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
7. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a power supply - AFF A800

Replacing a power supply involves disconnecting the target power supply (PSU) from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting it to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the red Fault LED on the power supply.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while

pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab
2	Power supply

5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

1. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - AFF A800

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where

the cables were connected.

Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

5. Remove the cable management device from the controller module and set it aside.
6. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

1. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

2. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 3: Remove the PCIe risers

You must remove one or more PCIe risers when replacing specific hardware components in the controller module.

1. Remove the PCIe riser from the controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward the fan modules.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.

1	Air duct
2	Riser 2 (middle riser) locking latch

Step 4: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

1. Locate the RTC battery under Riser 2.

1	Air duct
2	Riser 2
3	RTC battery and housing

2. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

3. Remove the replacement battery from the antistatic shipping bag.
4. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
5. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 5: Install the PCIe risers

You reinstall the PCIe risers after replacing the hardware components in the impaired controller.

1. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP modules that were removed from the PCIe cards.

Step 6: Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber

optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis.

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

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.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

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 X66240A-2 (112-00598), 2m X66240A-5 (112-00600), 5m		Network cable
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

Type of cable…	Part number and length	Connector type	For…
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 — Cabling a two-node switchless cluster

Step	Perform on each controller
1	Cable cluster interconnect ports: • Slot A4 and B4 (e4a) • Slot A8 and B8 (e8a)
2	Cable controller management (wrench) ports.

Step	Perform on each controller
3	Cable 25 GbE network switches: Ports in slot A3 and B3 (e3a and e3c) and slot A9 and B9 (e9a and e9c) to the 25 GbE network switches. 40GbE host network switches: Cable host-side b ports in slot A4 and B4 (e4b) and slot A8 and B8 (e8b) to the host switch.
4	Cable 32 Gb FC connections: 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.

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—Cabling a switched cluster

Step	Perform on each controller
1	Cable cluster interconnect a ports: • Slot A4 and B4 (e4a) to the cluster network switch. • Slot A8 and B8 (e8a) to the cluster network switch.
2	Cable controller management (wrench) ports.

Step	Perform on each controller
3	Cable 25GbE network switches: Ports in slot A3 and B3 (e3a and e3c) and slot A9 and B9 (e9a and e9c) to the 25 GbE network switches. 40GbE host network switches: Cable host-side b ports in slot A4 and B4 (e4b) and slot A8 and B8 (e8b) to the host switch.
4	Cable 32 Gb FC connecions: 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.

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—Cabling a single NS224 shelf

Step	Perform on each controller
1	• Connect controller A port e2a to port e0a on NSM A on the shelf. • Connect controller A port e10b to port e0b on NSM B on the shelf. 100 GbE cable

Step	Perform on each controller
2	• Connect controller B port e2a to port e0a on NSM B on the shelf. • Connect controller B port e10b to port e0b on NSM A on the shelf. 100 GbE cable

2. 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.

1. Use the following animation or diagram to cable your controllers to two NS224 drive shelves.

   Animation—Cabling two NS224 shelves

Shelf 1
Controller A
Slot 2
a
b
Slot 10
a
b
e0a
e0b
NSM A
e0a
e0b
NSM B
Shelf 2
Controller B
Slot 2
a
b
Slot 10
a
b
e0a
e0b
NSM A
e0a
e0b
NSM B

Shelf 1
NSM A
NSM B
Controller 1
Controller 2
Shelf 2
NSM A
NSM B

Step	Perform on each controller
1	• Connect controller A port e2a to NSM A e0a on shelf 1. • Connect controller A port e10b to NSM B e0b on shelf 1. • Connect controller A port e2b to NSM B e0b on shelf 2. • Connect controller A port e10a to NSM A e0a on shelf 2. 100 GbE cable
2	• Connect controller B port e2a to NSM B e0a on shelf 1. • Connect controller B port e10b to NSM A e0b on shelf 1. • Connect controller B port e2b to NSM A e0b on shelf 2. • Connect controller B port e10a to NSM B e0a on shelf 2. 100 GbE cable

2. To complete setting up your system, see Step 5: Complete system setup and configuration.

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: If network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

1. Use the following animation or drawing to set one or more drive shelf IDs:

   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—Setting 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—Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the ONTAP Configuration Guide.
8. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

b. Register your system.

   NetApp Product Registration

c. Download Active IQ Config Advisor.

   NetApp Downloads: Config Advisor

9. Verify the health of your system by running Config Advisor.
10. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: If network discovery is not enabled

If you are not using a Windows or Mac-based laptop or console or if auto discovery is not enabled, you must complete the configuration and setup using this task.

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the 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—Setting 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	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

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:
   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.
2. If you are not already grounded, properly ground yourself.
3. Remove the target slot blanking cover:
   a. Depress the lettered and numbered cam button.
   b. Rotate the cam latch down until it is the open position.
   c. Remove the blanking cover.
4. Install the I/O module:
   a. Align the I/O module with the edges of the slot.
   b. Slide the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
5. If the replacement I/O module is a NIC, cable the module to the data switches.

   > Make sure that any unused I/O slots have blanks installed to prevent possible thermal issues.

6. Reboot the 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 Migrating a LIF for information about using System Manager to permanently move the LIFs.
NIC I/O module with a storage I/O module	Use System Manager to permanently migrate the LIFs to different home ports, as described in Migrating a LIF.

2. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target 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.

      Removing 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 `storage port modify -node *<node name> -port *<port name> -mode network` command for each port.
Storage module	Install and cable your NS224 shelves, as described in Hot-adding an NS224 drive shelf.

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.

2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.

ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
     c. Shut down the impaired controller.
  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

     b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
     c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
     d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
     f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     g. Return to admin mode: `set -priv admin`
     h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager external sync`

     If the command fails, contact NetApp Support.

     mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. You can safely shut down the controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

     Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the impaired controller - 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 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller

storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Remove the controller, replace the boot media, and transfer the boot image - 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

❷	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

❶	Controller module cover locking button

Step 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 reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.
6. Reinstall the controller module lid by aligning the pins on the lid with the slots on the motherboard carrier, and then slide the lid into place.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the var file system during this procedure.

Before you begin

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Recable the controller module, as needed.
3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, and then push the cam handle to the closed position.

   The 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 iniitator adapter_name`
   c. Halt to return to Maintenance mode: `halt`

   The changes will be implemented when the system is booted.

Boot the recovery image - 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	a. Press `y` when prompted to restore the backup configuration. b. Press `y` when prompted to overwrite `/etc/ssh/ssh_host_ecdsa_key`. c. Press `y` when prompted to confirm if the restore backup was successful. d. Press `Y` when prompted to the restored configuration copy. e. Set the impaired controller to advanced privilege level: `set -privilege advanced` f. Run the restore backup command: `system node restore-backup -node local -target-address impaired_node_IP_address` g. Return the impaired controller to admin level: `set -privilege admin` h. Press `y` when prompted to use the restored configuration. i. Press `y` when prompted to reboot the impaired controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press `y`.

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 setenvenvironment_variable_name changed_value command.
   d. Save your changes using the saveenv command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Post boot media replacement steps for OKM, NSE, and NVE

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the boot_ontap command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the storage failover giveback -fromnode local command.
9. At the cluster prompt, check the logical interfaces with the net int -is-home false command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the net int revert command.

10. Move the console cable to the repaired 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).

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

Restore NVE or NSE when Onboard Key Manager is enabled

1. Connect the console cable to the target controller.
2. Use the boot_ontap command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`

If the console displays…	Then…
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager`, and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this section, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or security key-manager onboard show-backup` command.

   Example of backup data:

   Enter the backup data:


   ```
   --------------------------BEGIN BACKUP--------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   +
   --------------------------END BACKUP--------------------------
   ```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and log in as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer 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…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the storage failover giveback -fromnode local -only-cfo-aggregates true local command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner 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

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

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	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Move and replace hardware - 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	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. > You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the controller to normal operation.

If your system is running ONTAP…	Then…
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

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 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster

Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

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 reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 3: Move the system DIMMs

To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

1	DIMM ejector tabs
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	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev dev_name` dev_name can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev dev_name` After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev dev_name -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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode replacement_node_name` **Note:** If you disabled automatic giveback, re-enable it with the storage failover modify command.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. 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. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu. The controller module boots up when fully seated. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Recable the system - AFF A900

Continue the replacement procedure by recabling the storage and network conigurations.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

The system ID and disk assignment information reside in the NVRAM module, which is in a module separate from the controller module and not impacted by the controller module replacement.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

   ```
   node1> `storage failover show`
                                        Takeover
   Node              Partner            Possible     State Description
   ------------      ------------       --------
   -------------------------------------
   node1             node2              false        System ID changed on
   partner (Old:
                                                     151759755, New:
   151759706), In takeover
   node2             node1              -            Waiting for giveback
   (HA mailboxes)
   ```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node local-node-name partner savecore`
   c. Wait for the savecore command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

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  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node show`

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The 'metrocluster node show -fields node-systemid' command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* controller is the current owner of the disks on the disaster site.

     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

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a 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 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster

Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the terra cotta button on the cam handle downward until it unlocks.

   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 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.

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.

      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	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode replacement_node_name` **Note:** If you disabled automatic giveback, re-enable it with the storage failover modify command.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. c. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. d. Select Boot to maintenance mode from the menu. e. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. f. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the 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.

Safety Information and Regulatory Notices

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

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. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace 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 `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

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 `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Replace I/O modules

To replace an I/O module, locate it within the chassis and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Unplug any cabling associated with the target I/O module.

   Make sure that you label the cables so that you know where they came from.

3. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

   Make sure that you keep track of which slot the I/O module was in.

   Animation—Remove/install I/O module

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

4. Set the I/O module aside.
5. Install the replacement I/O module into the chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.
6. Recable the I/O module, as needed.

Step 3: Reboot the controller after I/O module replacement

After you replace an I/O module, you must reboot the controller module.

1. From the LOADER prompt, reboot the node: *bye*
2. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the nicadmin convert command from Maintenance mode.

   Be sure to exit Maintenance mode after completing the conversion.

3. Return the node to normal operation: `storage failover giveback -ofnode impaired_node_name`
4. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace 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

a. With the bezel removed, locate the LED USB module at the front of the chassis, on the bottom left side.
b. Slide the latch to partially eject the module.
c. Pull the module out of the bay to disconnect it from the midplane. Do not leave the slot empty.

2. Install the new LED USB module:
   a. Align the module to the bay with the notch in the corner of the module positioned near the slider latch on the chassis. The bay will prevent you from installing the module upside down.
   b. Push the module into the bay until it is fully seated flush with the chassis.

      There is an audible click when the module is secure and connected to the midplane.

Step 2: Return the failed component

1. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the 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 and NVRAM DIMM, you must remove the NVRAMmodule from th 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 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster

Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Replace the NVRAM module

To replace the NVRAM module, locate it in slot 6 in the chassis and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The NVRAM module disengages from the chassis and moves out a few inches.

   c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

      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`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node local-node-name partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

      The replacement controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      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  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node show`

   The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The replacement controller is the current owner of the disks on the disaster site.

     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

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

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.

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. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

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 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster

Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the terra cotta button on the cam handle downward until it unlocks.

   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

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

FAS systems

FAS500f System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick steps - FAS500f

This section gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

- English: FAS500f Installation and Setup Instructions
- Japanese: FAS500f Systems Installation and Setup Instructions
- Chinese: FAS500f Systems Installation and Setup Instructions

Videos - FAS500f

There are two videos - one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and Setup of a FAS500f

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed steps - FAS500f

This section gives detailed step-by-step instructions for installing a FAS500f system.

Step 1: Prepare for installation

To install your FAS500f system, you need to create an account and register the system. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the NetApp Hardware Universe (HWU) for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

What you need

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register (NetApp Product Registration) your system.
4. Download and install NetApp Downloads: Config Advisor on your laptop.
5. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the NetApp Hardware Universe to locate the cable and identify its use.

Type of cable…	Part number and length	Connector type	For…

25 GbE cable	X66240A-05 (112-00595), 0.5m; X66240-2 (112-00573), 2m		Cluster interconnect network
	X66240A-2 (112-00598), 2m; X66240A-5 (112-00600), 5m		Data
100 GbE cable	X66211-2 (112-00574), 2m; X66211-5 (112-00576), 5m		Storage
RJ-45 (order dependent)	Not applicable		Management network (BMC and wrench port) and Ethernet data (e0a and e0b)
Fibre Channel	X66250-2 (112-00342) 2m; X66250-5 (112-00344) 5m; X66250-15 (112-00346) 15m; X66250-30 (112-00347) 30m		
Micro-USB console cable	Not applicable		Console connection during software setup
Power cables	Not applicable		Powering up the system

1. Review the ONTAP Configuration Guide and collect the required information listed in that guide.

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

You need to be aware of the safety concerns associated with the weight of the system.

3. Identify and manage cables because this system does not have a cable management device.
4. Place the bezel on the front of the system.

Step 3: Cable controllers

There is required cabling for your platform's cluster using the two-node switchless cluster method or the cluster interconnect network method. There is optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cable to a host network and storage.

Required cabling: Cable controllers to a cluster

Cable the controllers to a cluster by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster

The management, Fibre Channel, and data or host network ports on the controller modules are connected to switches. The cluster interconnect ports are cabled on both controller modules.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cable a two-node switchless cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the 25GbE cluster interconnect cable : • e0c to e0c • e0d to e0d
2	Cable the wrench ports to the management network switches with the RJ45 cables.
!	DO NOT plug in the power cords at this point.

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 2: Cable a switched cluster

All ports on the controllers are connected to switches; cluster interconnect, management, Fibre Channel, and data or host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cabling a switched cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to the 25 GbE cluster interconnect switches. • e0c • e0d
2	Cable the wrench ports to the management network switches with the RJ45 cables.
!	DO NOT plug in the power cords at this point.

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Optional cabling: Cable configuration-dependent options

You have configuration-dependent optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cabling to a host network and storage.

Option 1: Cable to a Fibre Channel host network

Fibre Channel ports on the controllers are connected to Fibre Channel host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

+

Step	Perform on each controller module
1	Cable ports 2a through 2d to the FC host switches.
2	To perform other optional cabling, choose from: • Option 2: Cable to a 25GbE data or host network • Option 3: Cable the controllers to a single drive shelf
3	To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 2: Cable to a 25GbE data or host network

25GbE ports on the controllers are connected to 25GbE data or host network switches.

Before you begin

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Step	Perform on each controller module
1	Cable ports e4a through e4d to the 10GbE host network switches.
2	To perform other optional cabling, choose from: • Option 1: Cable to a Fibre Channel host network • Option 3: Cable the controllers to a single drive shelf
3	To complete setting up your system, see Step 4: Complete system setup and configuration.

Option 3: Cable the controllers to a single drive shelf

You must cable each controller to the NSM modules on the NS224 drive shelf.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation (Cabling the controllers to a single NS224) or the step-by-step instructions to cable your controller modules to a single shelf.

Step	Perform on each controller module
1	Cable controller A to the shelf:
2	Cable controller B to the shelf:

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

Step 4: Complete system setup and configuration

Complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Complete system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
2. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

3. Use the animation (Connecting your laptop to the Management switch) to connect your laptop to the Management switch.
4. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click **Network** in the left pane.
   c. Right-click and select **refresh**.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

5. Use System Manager guided setup to configure your system using the data you collected in the ONTAP Configuration Guide.
6. Verify the health of your system by running Config Advisor.
7. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Complete system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:

a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

> See your laptop or console's online help for how to configure the console port.

b. Connect the laptop or console to the switch on the management subnet.

c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

4. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

   > The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the ONTAP Configuration Guide.
5. Verify the health of your system by running Config Advisor.
6. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - FAS500f

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots.

You must have a USB flash drive, formatted to MBR/FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

Check onboard encryption keys - FAS500f

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.

4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the controller - FAS500f

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller. Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - FAS500f

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

   > If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

❶	Thumbscrew
❷	Controller module cover.

7. Lift out the air duct cover.

Step 2: Replace the boot media

You locate the failed boot media in the controller module by removing the air duct on the controller module before you can replace the boot media.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not loose it.

You can use the following video or the tabulated steps to replace the boot media:

Replacing the boot media

1. Locate and replace the impaired boot media from the controller module.

1	Remove the screw securing the boot media to the motherboard in the controller module.
2	Lift the boot media out of the controller module.

a. Using the #1 magnetic screwdriver, remove the screw from the impaired boot media, and set it aside safely on the magnet.
b. Gently lift the impaired boot media directly out of the socket and set it aside.
c. Remove the replacement boot media from the antistatic shipping bag and align it into place on the controller module.
d. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed is without a boot image so you need to transfer a boot image using a USB flash drive.

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the **Downloads** section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download

button.

  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.

- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
2. Download the service image to your work space on your laptop.
3. Unzip the service image.

   > If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

   There are two folders in the unzipped service image file:

   - `boot`
   - `efi`

4. Copy the `efi` folder to the top directory on the USB flash drive.

   The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

5. Remove the USB flash drive from your laptop.
6. If you have not already done so, install the air duct.

7. Close the controller module cover and tighten the thumbscrew.

❶	Controller module cover
❷	Thumbscrew

8. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
9. Plug the power cable into the power supply and reinstall the power cable retainer.
10. Insert the USB flash drive into the USB slot on the controller module.

    Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

11. Push the controller module all the way into the chassis:
12. Place your index fingers through the finger holes from the inside of the latching mechanism.
13. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
14. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

    The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

    The controller module should be fully inserted and flush with the edges of the chassis.

Boot the recovery image - FAS500f

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive:

   ```
   boot_recovery
   ```

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - FAS500f

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `storage failover show`-giveback` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.
7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.

- If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

  > If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - FAS500f

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - FAS500f

To replace the chassis, you must move the bezel, controller modules, and NVMe drives from the impaired chassis to the replacement chassis, and then remove the impaired chassis from the equipment rack or system cabinet and install the replacement chassis in its place.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the bezel, NVMe drives, and controller modules to the new chassis, and that the replacement chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - FAS500f

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or

a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

You can use the following video or the tabulated steps to replace the chassis; it assumes the removal and replacement of the bezel:

Replacing the chassis

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run

the diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

5. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - FAS500f

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:

   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

      - `ha`

    - `mcc`
    - `mccip`
    - `non-ha`
  b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test System** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - FAS500f

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.
- You must replace the failed component with a replacement FRU component you received from your provider.

- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - FAS500f

To shut down the impaired controller module, 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 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 content

- 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 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).

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the controller module hardware - FAS500f

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

You can use the following video or the tabulated steps to replace a controller module:

Replacing a controller module

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

❶	Thumbscrew
❷	Controller module cover.

7. Lift out the air duct cover.

Step 2: Move the power supply

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

1. Disconnect the power supply.
2. Open the power cable retainer, and then unplug the power cable from the power supply.
3. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

1	Blue power supply locking tab
2	Power supply

5. Move the power supply to the new controller module, and then install it.
6. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

Step 3: Move the fans

You must move the fans from the impaired controller module to the replacement module when replacing a failed controller module.

1. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan module

2. Move the fan module to the replacement controller module, and align the edges of the fan module with the opening in the controller module, and then slide the fan module in.
3. Repeat these steps for the remaining fan modules.

Step 4: Move the boot media

There is one boot media device in the AFF A250 under the air duct in the controller module. You must move it from the impaired controller module to the replacement controller module.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not lose it.

1. Locate and move the boot media from the impaired controller module to the replacement controller module.

1	Remove the screw securing the boot media to the motherboard in the impaired controller module.
2	Lift the boot media out of the impaired controller module.

a. Using the #1 magnetic screwdriver, remove the screw from the boot media, and set it aside safely on the magnet.
b. Gently lift the boot media directly out of the socket and align it into place in the replacement controller module.
c. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

Step 5: Move the DIMMs

To move the DIMMs, locate and move them from the impaired controller into the replacement controller and follow the specific sequence of steps.

+
image::../media/drw_a250_dimm_replace.png[]

+
IMPORTANT: Install each DIMM into the same slot it occupied in the impaired controller module.

1. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.

> Hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

2. Locate the corresponding DIMM slot on the replacement controller module.
3. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

4. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
5. Repeat these steps for the remaining DIMM.

Step 6: Move a mezzanine card

To move a mezzanine card, you must remove the cabling and any QSFPs and SFPs from the ports, move the mezzanine card to the replacement controller, reinstall any QSFPs and SFPs onto the ports, and cable the ports.

1. Locate and move the mezzanine cards from your impaired controller module.

1	Remove screws on the face of the controller module.

❷	Loosen the screw in the controller module.
❸	Move the mezzanine card.

2. Unplug any cabling associated with the mezzanine card.

   Make sure that you label the cables so that you know where they came from.

   a. Remove any SFP or QSFP modules that might be in the mezzanine card and set it aside.
   b. Using the #1 magnetic screwdriver, remove the screws from the face of the impaired controller module and from the mezzanine card, and set them aside safely on the magnet.
   c. Gently lift the mezzanine card out of the socket and move it to the same position in the replacement controller.
   d. Gently align the mezzanine card into place in the replacement controller.
   e. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the replacement controller module and on the mezzanine card.

   > Do not apply force when tightening the screw on the mezzanine card; you might crack it.

3. Repeat these steps if there is another mezzanine card in the impaired controller module.
4. Insert the SFP or QSFP modules that were removed onto the mezzanine card.

Step 7: Move the NV battery

When replacing the controller module, you must move the NV battery from the impaired controller module to the replacement controller module.

1. Locate and move the NVMEM battery from your impaired controller module to the replacement controller module.

1	Squeeze the clip on the face of the battery plug.
2	Unplug the battery cable from the socket.
3	Grasp the battery and press the blue locking tab marked PUSH.
4	Lift the battery out of the holder and controller module.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Locate the corresponding NV battery holder on the replacement controller module and align the NV battery to the battery holder.
5. Insert the NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

Step 8: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.

2. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

5. Insert the controller module into the chassis.
6. Ensure the latching mechanism arms are locked in the fully extended position.
7. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
8. Place your index fingers through the finger holes from the inside of the latching mechanism.
9. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
10. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching

mechanisms snap into place.

The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

The controller module should be fully inserted and flush with the edges of the chassis.

Restore and verify the system configuration - FAS500f

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the chassis

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - ha
   - mcc
   - mccip
   - non-ha

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test System** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

Recable the system and reassign disks - FAS500f

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                    Takeover
Node              Partner           Possible     State Description
------------      ------------      --------
-------------------------------------
node1             node2             false        System ID changed on
partner (Old:
                                                 151759755, New:
151759706), In takeover
node2             node1             -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

b. Save any coredumps: `system node run -node local-node-name partner savecore`

c. Wait for the `savecore`command to complete before issuing the giveback.

   You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      ⓘ If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration content for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node`

`show`

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* controller is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each controller is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each controller: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - FAS500f

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - FAS500f

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.

Step 3: Replace a DIMM

To replace a DIMM, you must locate it in the controller module using the DIMM map label on top of the air duct or locating it using the LED next to the DIMM, and then replace it following the specific sequence of steps.

You can use the following video or the tabulated steps to replace a DIMM:

Replacing a DIMM

1. Replace the impaired DIMM on your controller module.

   The DIMMs are in slot 3 or 1 on the motherboard. Slot 2 and 4 are left empty. Do not attempt to install DIMMs into these slots.

   The fault LED located on the board next to each DIMM blinks every two seconds.

2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
3. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.
4. Leave DIMM ejector tabs on the connector in the open position.
5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   > Hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

6. Insert the replacement DIMM squarely into the slot.

   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

7. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.

2. Close the controller module cover and tighten the thumbscrew.

❶	Controller module cover
❷	Thumbscrew

3. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   ⓘ You will connect the rest of the cables to the controller module later in this procedure.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF C190

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a fan — FAS500f

You replace a fan with a new fan module when it fails.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a fan module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever

with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover

Step 3: Replace a fan

To replace a fan, remove the failed fan module and replace it with a new fan module.

You can use the following video or the tabulated steps to replace a fan:

Replacing a fan

1. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
2. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.

1	Fan module

3. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace or install a mezzanine card - FAS500f

To replace a failed mezzanine card, you must remove the cables and any SFP or QSFP modules, replace the card, reinstall the SFP or QSFP modules and recable the cards. To install a new mezzanine card, you must have the appropriate cables and SFP or QSFP modules.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: System in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

Step 3: Replace or install a mezzanine card

To replace a mezzanine card, you must remove the impaired card and install the replacement card; to install a mezzanine card, you must remove the faceplate and install the new card.

You can use the following video or the tabulated steps to replace a mezzanine card:

Replacing a mezzanine card

Option 1: Replace a mezzanine card:

1. Locate and replace the impaired mezzanine card on your controller module.

1	Remove screws on the face of the controller module.
2	Loosen the screw in the controller module.
3	Remove the mezzanine card.

2. Unplug any cabling associated with the impaired mezzanine card.

   Make sure that you label the cables so that you know where they came from.

3. Remove any SFP or QSFP modules that might be in the impaired mezzanine card and set it aside.
4. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and set them aside safely on the magnet.
5. Using the #1 magnetic screwdriver, loosen the screw on the impaired mezzanine card.
6. Using the #1 magnetic screwdriver, gently lift the impaired mezzanine card directly out of the socket and set it aside.
7. Remove the replacement mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.
8. Gently align the replacement mezzanine card into place.
9. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

Do not apply force when tightening the screw on the mezzanine card; you might crack it.

10. Insert any SFP or QSFP modules that were removed from the impaired mezzanine card to the replacement mezzanine card.

Option 2: Install a mezzanine card:

You install a new mezzanine card if your system does not have one.
. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and the faceplate covering the mezzanine card slot, and set them aside safely on the magnet.
. Remove the mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.
. Gently align the mezzanine card into place.
. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

+
NOTE: Do not apply force when tightening the screw on the mezzanine card; you might crack it.

Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.

❶	Controller module cover
❷	Thumbscrew

2. Insert the controller module into the chassis

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - FAS500f

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module.

You can use the following video or the tabulated steps to replace the NVMEM battery:

Replacing the NVMEM battery

1. Locate and replace the impaired NVMEM battery on your controller module.

   It is recommended that you follow the illustrated instructions in the order listed.

1	Squeeze the clip on the face of the battery plug.
2	Unplug the battery cable from the socket.

❸	Grasp the battery and press the blue locking tab marked PUSH.
❹	Lift the battery out of the holder and controller module.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module and set it aside.
4. Remove the replacement NV battery from the antistatic shipping bag and align it to the battery holder.
5. Insert the replacement NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. Close the controller module cover and tighten the thumbscrew.

1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select Reboot from the menu to reboot the system.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a power supply - FAS500f

Replacing a power supply involves disconnecting the target power supply (PSU) from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting it to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

You can use the following video or the tabulated steps to replace the power supply:

Replacing the power supply

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the red Fault LED on the power supply.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.

1	Blue power supply locking tab
2	Power supply

5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

> To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

7. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

Make sure that you label the cables so that you know where they came from.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.

Step 3: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

You can use the following video or the tabulated steps to replace the RTC battery:

Replacing the RTC battery

1. Locate the RTC battery between the heatsink and the midplane and remove it exactly as shown in the graphic.

1	Gently pull tab away from the battery housing. NOTE: Pulling it away aggressively might displace the tab.
2	Lift the battery up. Make a note of the polarity of the battery.
3	The battery should eject out.

The battery will be ejected out.

2. Remove the replacement battery from the antistatic shipping bag.
3. Locate the RTC battery holder between the heatsink and the midplane and insert it exactly as shown in the graphic.

1	With positive polarity face up, slide the battery under the tab of the battery housing.
2	Push the battery gently into place and make sure the tab secures it to the housing. + **CAUTION:** + Pushing it in aggressively might cause the battery to eject out again.

4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and set time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

Steps

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller

module halfway into the system.

Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   f. Halt the controller at the LOADER prompt.

   The controller module should be fully inserted and flush with the edges of the chassis.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Complete the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

FAS2600 System Documentation

Install and setup

Cluster configuration worksheet - FAS2600

You can use the worksheet to gather and record your site-specific IP addresses and other information required when configuring an ONTAP cluster.

Cluster Configuration Worksheet

Start here: Choose your installation and setup experience

You can choose from different content formats to guide you through installing and setting up your new storage system.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

Installation and setup PDF poster - FAS2600

You can use the PDF poster to install and set up your new system. The AFF FAS2600 Installation and Setup Instructions provides step-by-step instructions with live links to additional content.

Installation and setup video - FAS2600

The following video shows end-to-end software configuration for systems running ONTAP 9.2.

AFF FAS2600 Setup Video

Maintain

Boot media

Overview of boot media replacement - FAS2600

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:

- For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
- For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.

- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys - FAS2600

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy

controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes` manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers

display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        > Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`

   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.

- If no disks are shown, NSE is not configured.
- If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
     c. Shut down the impaired controller.
  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager onboard`

`sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

Shut down the impaired controller - FAS2600

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.

If the impaired controller displays…	Then…
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Replace the boot media - FAS2600

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Replace the boot media

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:

3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

4. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
5. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the var file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired controller from the healthy controller during var file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.
     - dns_addr is the IP address of a name server on your network.
     - dns_domain is the Domain Name System (DNS) domain name.

       If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

     > Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

Boot the recovery image - FAS2600

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenvenvironment_variable_name changed_value` command.
   d. Save your changes using the `saveenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - FAS2600

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


   ```
   ---------------------------BEGIN BACKUP---------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   ---------------------------END BACKUP---------------------------
   ```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int`

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   > This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - FAS2600

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module - FAS2600

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

- You must replace the failed component with a replacement FRU component you received from your provider.

AFF FAS2600 caching module replacement video

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

About this task

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller.

ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run`
   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

The output should display the caching module status as erased.

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace a caching module

To replace a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

1. Locate the caching module at the rear of the controller module and remove it.
   a. Press the release tab.
   b. Remove the heatsink.

1. Gently pull the caching module straight out of the housing.
2. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
3. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

4. Reseat and push the heatsink down to engage the locking button on the caching module housing.
5. Close the controller module cover, as needed.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

1. If you have not already done so, replace the cover on the controller module.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`
4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation: **If your controller is in an HA pair**, perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* **Note:** If you disabled automatic giveback, re-enable it with the `storage failover modify` command. **If your controller is in a stand-alone configuration**, proceed to the next step. No action is required. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - FAS2600

To replace the chassis, you must move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the

same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

AFF FAS2600 chassis replacement video

Shut down the controllers - FAS2600

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

> You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node *second_node_name* -ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Move and replace hardware - FAS2600

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Move the power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.
4. Use the cam handle to slide the power supply out of the system.

> When removing a power supply, always use two hands to support its weight.

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   > Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

   > Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

Step 2: Remove the controller module

Remove the controller module or modules from the old chassis.

1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

2. Remove and set aside the cable management devices from the left and right sides of the controller module.

3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

4. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 3: Move drives to the new chassis

Move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 4: Replace a chassis from within the equipment rack or system cabinet

Remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Repeat the preceding steps for the second controller module in the new chassis.
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Reinstall the blanking panel and then go to the next step.

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

      If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

   b. From the boot menu, select the option for Maintenance mode.

Restore and verify the configuration - FAS2600

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

      - `ha`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. The next step depends on your system configuration.

If your system is in…	Then…
A stand-alone configuration	a. Exit Maintenance mode: `halt` b. Go to "Completing the replacement process.
An HA pair with a second controller module	Exit Maintenance mode: `halt` The LOADER prompt appears.

Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

> Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. > You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the controller to normal operation:

If your system is running ONTAP…	Then…
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command: `node::> storage failover modify -node node0 -enabled true`
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - FAS2600

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system’s configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the controller - FAS2600

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Replace the controller module hardware - FAS2600

To replace the controller module, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

AFF FAS2600 controller replacement video

Step 1: Remove controller module

To replace the controller module, you must first remove the old controller module from the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

6. Turn the controller module over and place it on a flat, stable surface.
7. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Move the boot media

You must locate the boot media and follow the directions to remove it from the old controller module and insert it in the new controller module.

Steps

1. Locate the boot media using the following illustration or the FRU map on the controller module:

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

   Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 3: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

Steps

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

- If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
- If the LED is on and power is on, unwritten data is stored on NVMEM.

  This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

Steps

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

   > Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

   The number and placement of system DIMMs depends on the model of your system.

   The following illustration shows the location of system DIMMs:

4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

   Make sure that the plug locks down onto the controller module.

Step 5: Move the caching module

To move a caching module referred to as the M.2 PCIe card on the label on your controller, locate and move it from the old controller into the replacement controller and follow the specific sequence of steps.

You must have the new controller module ready so that you can move the caching module directly from the old controller module to the corresponding slot in the new one. All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. Locate the caching module at the rear of the controller module and remove it.

   a. Press the release tab.

   b. Remove the heatsink.

2. Gently pull the caching module straight out of the housing.
3. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Close the controller module cover, as needed.

Step 6: Install the controller

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Important: During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

Restore and verify the system configuration - FAS2600

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device..
   - `cna` is a Converged Network Adapter or interface not connected to a network or storage device.
   - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - `mem` is system memory.
   - `nic` is a network interface card.
   - `nvram` is nonvolatile RAM.
   - `nvmem` is a hybrid of NVRAM and system memory.
   - `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`* *dev_name* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev` *`dev_name`* After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - FAS2600

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.
You must use the correct procedure for your configuration.

Option 1: Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch: `boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node local-node-name partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. Verify that the expected volumes are present for each controller: `vol show -node node-name`

8. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

Option 2: Manually reassign the system ID on a stand-alone system in ONTAP

In a stand-alone system, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems that are in a stand-alone configuration.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.
2. You must enter `Y` when prompted to override the system ID due to a system ID mismatch.
3. View the system IDs: `disk show -a`
4. You should make a note of the old system ID, which is displayed as part of the disk owner column.

   The following example shows the old system ID of 118073209:

```
*> disk show -a
Local System ID: 118065481

  DISK      OWNER                   POOL   SERIAL NUMBER  HOME
--------    -------------           -----  -------------  -------------
disk_name    system-1  (118073209)  Pool0  J8XJE9LC       system-1
(118073209)
disk_name    system-1  (118073209)  Pool0  J8Y478RC       system-1
(118073209)
.
.
.
```

5. Reassign disk ownership by using the system ID information obtained from the disk show command: `disk reassign -s old system ID disk reassign -s 118073209`
6. Verify that the disks were assigned correctly: `disk show -a`

   The disks belonging to the replacement node should show the new system ID. The following example now show the disks owned by system-1 the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK      OWNER                   POOL   SERIAL NUMBER  HOME
--------    -------------           -----  -------------  -------------
disk_name    system-1  (118065481)  Pool0  J8Y0TDZC       system-1
(118065481)
disk_name    system-1  (118065481)  Pool0  J8Y0TDZC       system-1
(118065481)
.
.
.
```

7. Boot the node: `boot_ontap`

Complete system restoration - FAS2600

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

> The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and register the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - FAS2600

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a

system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

AFF FAS2600 DIMM replacement video

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

1. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

2. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
3. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:
   a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.

b. Confirm that the NVMEM LED is no longer lit.

c. Reconnect the battery connector.

4. Recheck the NVMEM LED.
5. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

6. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
7. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

8. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

9. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

10. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
11. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

12. Close the controller module cover.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

1. If you have not already done so, replace the cover on the controller module.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	**Then…**
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - FAS2600

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - FAS2600

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

AFF FAS2600 NVMEM battery replacement video

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Remove the battery from the controller module and set it aside.
5. Remove the replacement battery from its package.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.

8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
9. Plug the battery plug back into the controller module.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

1. If you have not already done so, replace the cover on the controller module.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - FAS2600

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

AFF FAS2600 power supply replacement video

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

5. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. Reconnect the power supply cabling:

   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

10. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

    The power supply LEDs are lit when the power supply comes online.

11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

AFF FAS2600 RTC battery replacement video

Step 1: Shut down the impaired controller

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

1. Locate the RTC battery.

2. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

3. Remove the replacement battery from the antistatic shipping bag.
4. Locate the empty battery holder in the controller module.
5. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
6. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and set time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Complete the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

FAS2700 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick guide - AFF A220 and FAS2700

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A220/FAS2700 Systems Installation and Setup Instructions

Videos - AFF A220 and FAS2700

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

NetApp video: AFF A220 and FAS2700 Systems: Installation and Setup Instructions

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - AFF A220 and FAS2700

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Step 1: Prepare for installation

To install your FAS2700 or AFF A220 system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific

network information.

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
- A laptop or console with an RJ-45 connection and access to a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register your system.

      NetApp Product Registration

4. Download and install Config Advisor on your laptop.

   NetApp Downloads: Config Advisor

5. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
10 GbE cable (order dependent)	X6566B-05-R6 (112-00297), 0.5m X6566B-2-R6 (112-00299), 2m		Cluster interconnect network

Type of cable…	Part number and length	Connector type	For…
10 GbE cable (order dependent)	Part number X6566B-2-R6 (112-00299), 2m or X6566B-3-R6 (112-00300), 3m X6566B-5-R6 (112-00301), 5m		Data
Optical network cables (order dependent)	X6553-R6 (112-00188), 2m X6536-R6 (112-00090), 5m X6554-R6(112-00189), 15m		FC host network
Cat 6, RJ-45 (order dependent)	Part numbers X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network and Ethernet data
Storage (order dependent)	Part number X66030A (112-00435), 0.5m X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		Storage
Micro-USB console cable	Not applicable		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	Not applicable		Powering up the system

6. Download and complete the *Cluster configuration worksheet*.

   Cluster Configuration Worksheet

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.

3. Attach cable management devices (as shown).

4. Place the bezel on the front of the system.

Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster, unified network configuration

Management network, UTA2 data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the cluster interconnect cable: • e0a to e0a • e0b to e0b

Step	Perform on each controller
2	Use one of the following cable types to cable the UTA2 data ports to your host network: An FC host • 0c and 0d • **or** 0e and 0f A 10GbE • e0c and e0d • **or** e0e and e0f You can connect one port pair as CNA and one port pair as FC, or you can connect both port pairs as CNA or both port pairs as FC.
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Option 2: Cable a switched cluster, unified network configuration

Management network, UTA2 data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and the switches:

Step	Perform on each controller module
1	Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:
2	Use one of the following cable types to cable the UTA2 data ports to your host network: An FC host • 0c and 0d • **or** 0e and 0f A 10GbE • e0c and e0d • **or** e0e and e0f ⓘ You can connect one port pair as CNA and one port pair as FC, or you can connect both port pairs as CNA or both port pairs as FC.

Step	Perform on each controller module
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Option 3: Cable a two-node switchless cluster, Ethernet network configuration

Management network, Ethernet data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and to the switches:

Step	Perform on each controller
1	Cable the cluster interconnect ports to each other with the cluster interconnect cable: • e0a to e0a • e0b to e0b
2	Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:

Step	Perform on each controller
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Option 4: Cable a switched cluster, Ethernet network configuration

Management network, Ethernet data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and the switches:

Step	Perform on each controller module
1	Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:
2	Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:

Step	Perform on each controller module
3	Cable the e0M ports to the management network switches with the RJ45 cables:
!	DO NOT plug in the power cords at this point.

2. To cable your storage, see Cabling controllers to drive shelves

Step 4: Cable controllers to drive shelves

You must cable the controllers to your shelves using the onboard storage ports. NetApp recommends MP-HA cabling for systems with external storage. If you have a SAS tape drive, you can use single-path cabling. If you have no external shelves, MP-HA cabling to internal drives is optional (not shown) if the SAS cables are ordered with the system.

Option 1: Cable storage on an HA pair with external drive shelves

You must cable the shelf-to-shelf connections, and then cable both controllers to the drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

Steps

1. Cable the HA pair with external drive shelves:

> The example uses DS224C. Cabling is similar with other supported drive shelves.

Step	Perform on each controller
1	Cable the shelf-to-shelf ports. • Port 3 on IOM A to port 1 on the IOM A on the shelf directly below. • Port 3 on IOM B to port 1 on the IOM B on the shelf directly below. mini-SAS HD to mini-SAS HD cables
2	Connect each node to IOM A in the stack. • Controller 1 port 0b to IOM A port 3 on last drive shelf in the stack. • Controller 2 port 0a to IOM A port 1 on the first drive shelf in the stack. mini-SAS HD to mini-SAS HD cables
3	Connect each node to IOM B in the stack • Controller 1 port 0a to IOM B port 1 on first drive shelf in the stack. • Controller 2 port 0b to IOM B port 3 on the last drive shelf in the stack. mini-SAS HD to mini-SAS HD cables

If you have more than one drive shelf stack, see the *Installation and Cabling Guide* for your drive shelf type.

Installing and cabling

2. To complete setting up your system, see Completing system setup and configuration

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Complete system setup if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Use the following animation to set one or more drive shelf IDs

   Setting drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

> Initial booting may take up to eight minutes.

4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:

a. Open File Explorer.
b. Click network in the left pane.
c. Right click and select refresh.
d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

> XXXXX is the system serial number for the target node.

System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

   ONTAP Configuration Guide

8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

   > See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console, and connect the console port on the controller using the console cable that came with your system.

c. Connect the laptop or console to the switch on the management subnet.

d. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.

2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.

If the management network has DHCP…	Then…
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

7. Verify the health of your system by running Config Advisor.
8. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A220 and FAS2700

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.

- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys - AFF A220 and FAS2700

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes` manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to back up the OKM information: `security key-manager backup show`

> Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

- Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. Shut down the impaired controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. Shut down the impaired controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager external sync`

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. You can safely shut down the controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the impaired controller - AFF A220 and FAS2700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.

If the impaired controller displays…	Then…
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A220 and FAS2700

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Replace the boot media

You must locate the boot media in the controller and follow the directions to replace it.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:

3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

4. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
5. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the var file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.

- If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.

- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired controller from the healthy controller during var file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.
     - dns_addr is the IP address of a name server on your network.
     - dns_domain is the Domain Name System (DNS) domain name.

If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

> Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

Boot the recovery image - AFF A220 and FAS2700

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.

d. Save your changes using the `savenv` command.

5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.
10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore OKM, NSE, and NVE as needed - AFF A220 and FAS2700

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:

```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.

b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

> If the `Restored` column = anything other than `yes`, contact Customer Support.

c. Wait 10 minutes for the key to synchronize across the cluster.

14. If you are running ONTAP 9.6 or later:

    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.

    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

    > If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.

15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.

If the console displays…	Then…
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.
   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A220 and FAS2700

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module - AFF A220 and FAS2700

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

- You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller.

+
ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

Steps

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run`
   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

      The output should display the caching module status as erased.
2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

4. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace a caching module

To replace a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the caching module at the rear of the controller module and remove it.

   a. Press the release tab.

   b. Remove the heatsink.

3. Gently pull the caching module straight out of the housing.
4. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
5. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

6. Reseat and push the heatsink down to engage the locking button on the caching module housing.

7. Close the controller module cover, as needed.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>)

appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`
4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

1. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation: **If your controller is in an HA pair**, perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* **Note:** If you disabled automatic giveback, re-enable it with the `storage failover modify` command. **If your controller is in a stand-alone configuration**, proceed to the next step. No action is required. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A220 and FAS2700

To replace the chassis, you must move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A220 and FAS2700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Controller is in a MetroCluster configuration

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Move and replace hardware - AFF A220 and FAS2700

Move the power supplies, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Move a power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

4. Use the cam handle to slide the power supply out of the system.

> When removing a power supply, always use two hands to support its weight.

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

> Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

> Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

Step 2: Remove the controller module

Remove the controller module or modules from the old chassis.

1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

2. Remove and set aside the cable management devices from the left and right sides of the controller module.

3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

4. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 3: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

      When removing a drive, always use two hands to support its weight.

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It click when it is secure.
6. Repeat the process for the remaining drives in the system.

Step 4: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.
2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Repeat the preceding steps for the second controller module in the new chassis.
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Reinstall the blanking panel and then go to the next step.

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

      If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

   b. From the boot menu, select the option for Maintenance mode.

Restore and verify the configuration - AFF A220 and FAS2700

You must verify the HA state of the chassis and run System-Level diagnostics, switch back aggregates, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis HA-state`

      The value for HA-state can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. The next step depends on your system configuration.

If your system is in…	Then…
A stand-alone configuration	a. Exit Maintenance mode: `halt` b. Go to "Completing the replacement process.
An HA pair with a second controller module	Exit Maintenance mode: `halt` The LOADER prompt appears.

Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the controller to normal operation:

If your system is running ONTAP…	Then…
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If your system is running ONTAP…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - AFF A220 and FAS2700

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

  If this is the procedure you should use, note that the controller replacement procedure for a controller in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific

steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system's configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - AFF A220 and FAS2700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=_number_of_hours_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module..
Waiting for giveback…	Press Ctrl-C, and then respond `y`.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the controller module hardware - AFF A220 and FAS2700

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove controller module

To replace the controller module, you must first remove the old controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

6. Turn the controller module over and place it on a flat, stable surface.
7. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 2: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.

7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

Step 3: Move the boot media

You must locate the boot media and follow the directions to remove it from the old controller module and insert it in the new controller module.

1. Locate the boot media using the following illustration or the FRU map on the controller module:

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired

controller module to the corresponding slots in the replacement controller module.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

   > Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

   The number and placement of system DIMMs depends on the model of your system.

   The following illustration shows the location of system DIMMs:

4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

Make sure that the plug locks down onto the controller module.

Step 5: Move a caching module, if present

If your AFF A220 or FAS2700 system has a caching module, you need to move the caching module from the old controller module to the replacement controller module. The caching module is referred to as the “M.2 PCIe card” on the controller module label.

You must have the new controller module ready so that you can move the caching module directly from the old controller module to the corresponding slot in the new one. All other components in the storage system must be functioning properly; if not, you must contact technical support.

1. Locate the caching module at the rear of the controller module and remove it.

   a. Press the release tab.

   b. Remove the heatsink.

2. Gently pull the caching module straight out of the housing.
3. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Close the controller module cover, as needed.

Step 6: Install the controller

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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; you might damage the connectors. The controller begins to boot as soon as it is seated in the chassis. 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. Interrupt the boot process **only** after determining the correct timing: You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete. Only press `Ctrl-C` when you see the message `Press Ctrl-C for Boot Menu`. ⓘ If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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. Interrupt the boot process **only** after determining the correct timing: You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete. Only press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. f. From the boot menu, select the option for Maintenance mode.

Important: During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

    - `ha`
    - `mcc`
    - `mcc-2n`
    - `mccip`
    - `non-ha`

  b. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device..
   - cna is a Converged Network Adapter or interface not connected to a network or storage device.
   - fcal is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - mem is system memory.
   - nic is a network interface card.
   - `nvram` is nonvolatile RAM.
   - `nvmem` is a hybrid of NVRAM and system memory.
   - `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`* *dev_name* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev` *`dev_name`* After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - AFF A220 and FAS2700

To complete the replacement procedure and restore your system to full operation, you must recable the storage, confirm disk reassignment, restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller. You must complete a series of tasks before restoring your system to full operation.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.

c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.

You must use the correct procedure for your configuration:

Controller redundancy	Then use this procedure…
HA pair	Verifying the system ID change on an HA system
Stand-alone	Manually reassigning the system ID on a stand-alone system in ONTAP
Two-node MetroCluster configuration	Manually reassigning the system ID on systems in a two-node MetroCluster configuration

Option 1: Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node` *`local-node-name`* `partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration content for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

Option 2: Manually reassign the system ID on a stand-alone system in ONTAP

In a stand-alone system, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

> **About this task**
> This procedure applies only to systems that are in a stand-alone configuration.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.
2. You must enter `Y` when prompted to override the system ID due to a system ID mismatch.
3. View the system IDs: `disk show -a`
4. You should make a note of the old system ID, which is displayed as part of the disk owner column.

   The following example shows the old system ID of 118073209:

```
*> disk show -a
Local System ID: 118065481

  DISK      OWNER                  POOL   SERIAL NUMBER  HOME
--------    -------------          -----  -------------  -------------
disk_name    system-1  (118073209)  Pool0  J8XJE9LC       system-1
(118073209)
disk_name    system-1  (118073209)  Pool0  J8Y478RC       system-1
(118073209)
.
.
.
```

5. Reassign disk ownership by using the system ID information obtained from the disk show command: `disk reassign -s old system ID disk reassign -s 118073209`
6. Verify that the disks were assigned correctly: `disk show -a`

   The disks belonging to the replacement node should show the new system ID. The following example now show the disks owned by system-1 the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK      OWNER                   POOL   SERIAL NUMBER  HOME
--------    -------------           -----  -------------  -------------
disk_name    system-1  (118065481)  Pool0  J8Y0TDZC       system-1
(118065481)
disk_name    system-1  (118065481)  Pool0  J8Y0TDZC       system-1
(118065481)
.
.
.
```

7. Boot the node: `boot_ontap`

Option 3: Manually reassign the system ID on systems in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering `Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid`,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

```
dr-group-id cluster         node                 node-systemid dr-
partner-systemid
 ----------- --------------------- -------------------- -------------
-------------------
 1           Cluster_A             Node_A_1             536872914
118073209
 1           Cluster_B             Node_B_1             118073209
536872914
 2 entries were displayed.
```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

```
Local System ID: 118065481
    ...
    ...
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                 POOL   SERIAL NUMBER  HOME
-------    -------------         -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:

a. Change to the advanced privilege level: `set -privilege advanced`

   You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

b. Verify that the coredumps are saved: `system node run -node local-node-name partner savecore`

   If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node local-node-name partner savecore -s command`.</info>.

c. Return to the admin privilege level: `set -privilege admin`

7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`

c. Return to the admin privilege level: `set -privilege admin`

Complete system restoration - AFF A220 and FAS2700

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption

functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and register the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - AFF A220 and FAS2700

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Steps

1. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
2. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

3. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

3. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
4. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:

a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.

b. Confirm that the NVMEM LED is no longer lit.

c. Reconnect the battery connector.

5. Return to Replace the DIMMs of this procedure to recheck the NVMEM LED.
6. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

7. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
8. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

9. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

10. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

    The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

    Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

11. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
12. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

13. Close the controller module cover.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. > If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace SSD Drive or HDD Drive - AFF A220 and FAS2700

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

Option 1: Replace SSD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - AFF A220 and FAS2700

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

4. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
5. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt` *`impaired_node_name`*

6. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired controller's power cords from the power source.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller

module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

Steps

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

3. Locate the NVMEM battery in the controller module.

4. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
5. Remove the battery from the controller module and set it aside.
6. Remove the replacement battery from its package.
7. Loop the battery cable around the cable channel on the side of the battery holder.
8. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
9. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
10. Plug the battery plug back into the controller module.

Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

4. Recable the system, as needed.

If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process. 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. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A220 and FAS2700

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

- Power supplies are auto-ranging.

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

5. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. Reconnect the power supply cabling:

   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

10. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

    The power supply LEDs are lit when the power supply comes online.

11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a two-node MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Step 2: Remove controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

Step 3: Replace the RTC battery

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and set time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

FAS8200 System Documentation

Install and setup

Cluster configuration worksheet - FAS8200

You can use the Cluster Configuration Worksheet to gather and record your site-specific IP addresses and other information required when configuring an ONTAP cluster.

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

Installation and setup PDF poster - FAS8200

You can use the PDF poster to install and set up your new system. The AFF FAS8200 Installation and Setup Instructions provides step-by-step instructions with live links to additional content.

Installation and setup video - FAS8200

The following video shows end-to-end software configuration for systems running ONTAP 9.2.

AFF FAS8200 Setup Video

Maintain

Boot media

Overview of boot media replacement - FAS8200

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption - FAS8200

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`

   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.

- If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

   c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        > Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Restore the external key management authentication keys to all nodes in the cluster: `security`

`key-manager external restore`

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.
After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster configuration

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node Metrocluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the boot media - FAS8200

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	
Thumbscrew	
2	
Cam handle	

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 2: Replace the boot media

You must locate the boot media in the controller and follow the directions to replace it.

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:

3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

4. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
5. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the var file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.

- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired controller from the healthy controller during var file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.

- dns_addr is the IP address of a name server on your network.
- dns_domain is the Domain Name System (DNS) domain name.

  If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

> Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

8. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:
   a. Boot to Maintenance mode: `boot_ontap maint`
   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t` *`initiator adapter_name`*
   c. Halt to return to Maintenance mode: `halt`

The changes will be implemented when the system is booted.

Boot the recovery image - FAS8200

The procedure for booting the impaired controller from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1: Most systems

:
You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

If you see…	Then…
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.

8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Controller is in a two-node MetroCluster

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. After the image is installed, start the restoration process:
   a. Press `n` when prompted to restore the backup configuration.
   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
   e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - FAS8200

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - FAS8200

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.

- If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - FAS8200

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module - FAS8200

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure

to do so results in performance degradation.

You might want to erase the contents of your caching module before replacing it.
. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
.. Erase the data on the caching module: `system controller flash-cache secure-erase run`
.. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

+
The output should display the caching module status as erased.

- You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace or add a caching module

To replace or add a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slots inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

  1. Locate the caching module at the rear of the controller module and remove it.
     a. Press the release tab.
     b. Remove the heatsink.

The storage system comes with two slots available for the caching module and only one slot is occupied, by default.

2. If you are adding a caching module, go to the next step; if you are replacing the caching module, gently pull it straight out of the housing.
3. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Repeat the steps if you have a second caching module. Close the controller module cover, as needed.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

3. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`

4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	Then…
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Complete the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - FAS8200

To replace the chassis, you must move the power supplies, fans, and controller modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - FAS8200

To replace the chassis, you must shutdown the controllers.

Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Controller is in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace hardware - FAS8200

Move the power supplies, fans, and controller modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Move a power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.

b. Open the power cable retainer, and then unplug the power cable from the power supply.

c. Unplug the power cable from the power source.

3. Press down the release latch on the power supply cam handle, and then lower the cam handle to the fully open position to release the power supply from the mid plane.

1	Power supply
2	Cam handle release latch

3	Power and Fault LEDs
4	Cam handle
5	Power cable locking mechanism

4. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

5. Repeat the preceding steps for any remaining power supplies.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Push firmly on the power supply cam handle to seat it all the way into the chassis, and then push the cam handle to the closed position, making sure that the cam handle release latch clicks into its locked position.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

   Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

Step 2: Move a fan

Moving out a fan module when replacing the chassis involves a specific sequence of tasks.

1. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
2. Press down the release latch on the fan module cam handle, and then pull the cam handle downward.

   The fan module moves a little bit away from the chassis.

1	Cam handle
2	Fan module
3	Cam handle release latch
4	Fan module Attention LED

3. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

4. Set the fan module aside.
5. Repeat the preceding steps for any remaining fan modules.
6. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.
7. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

8. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

9. Repeat these steps for the remaining fan modules.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Step 3: Remove the controller module

To replace the chassis, you must remove the controller module or modules from the old chassis.

1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

2. Remove and set aside the cable management devices from the left and right sides of the controller module.

3. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

4. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 4: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.

   If the system is in a system cabinet, you might need to remove the rear tie-down bracket.

2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. 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. Repeat the preceding steps for the second controller module in the new chassis.
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. 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. Reinstall the blanking panel and then go to the next step.

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

      If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

   b. From the boot menu, select the option for Maintenance mode.

Restore and verify the configuration - FAS8200

You must verify the HA state of the chassis and run System-Level diagnostics, switch back aggregates, and return the failed part to NetApp, as described in the RMA

instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:
      * **`ha`**
      * `mcc`
      * **`mcc-2n`**
      * `mccip`
      * `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. The next step depends on your system configuration.

If your system is in…	Then…
A stand-alone configuration	a. Exit Maintenance mode: `halt` b. Go to "Completing the replacement process.
An HA pair with a second controller module	Exit Maintenance mode: `halt` The LOADER prompt appears.

Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the controller to normal operation:

If your system is running ONTAP…	Then…
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If your system is running ONTAP…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overiew of controller module replacement - FAS8200

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is a FlexArray system or has a V_StorageAttach license, you must refer to the additional required steps before performing this procedure.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

If this is the procedure you should use, note that the controller replacement procedure for a controller in a four or eight controller MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system's configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- Any PCIe cards moved from the old controller module to the new controller module or added from existing customer site inventory must be supported by the replacement controller module.

  NetApp Hardware Universe

- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - FAS8200

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message`

`MAINT=_number_of_hours_down_h`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module..
Waiting for giveback…	Press Ctrl-C, and then respond `y`.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the controller module hardware - FAS8200

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Open the controller module

To replace the controller module, you must first remove the old controller module from the chassis.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

6. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 2: Move the boot device

You must locate the boot media and follow the directions to remove it from the old controller and insert it in the new controller.

1. Locate the boot media using the following illustration or the FRU map on the controller module:

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

   > Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 3: Move the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.

- If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

  - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
  - If the LED is on and power is on, unwritten data is stored on NVMEM.

    This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Open the CPU air duct and locate the NVMEM battery.

1	Battery lock tab
2	NVMEM battery pack

3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Remove the battery from the controller module and set it aside.

Step 4: Move the DIMMs

To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

   > Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

   The number and placement of system DIMMs depends on the model of your system.

   The following illustration shows the location of system DIMMs:

4. Locate the slot where you are installing the DIMM.
5. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Repeat these steps for the remaining DIMMs.
7. Move the NVMEM battery to the replacement controller module.
8. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.

Step 5: Move a PCIe card

To move PCIe cards, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

You must have the new controller module ready so that you can move the PCIe cards directly from the old controller module to the corresponding slots in the new one.

1. Loosen the thumbscrew on the controller module side panel.
2. Swing the side panel off the controller module.

1	
Side panel	
2	
PCIe card	

3. Remove the PCIe card from the old controller module and set it aside.

   Make sure that you keep track of which slot the PCIe card was in.

4. Repeat the preceding step for the remaining PCIe cards in the old controller module.
5. Open the new controller module side panel, if necessary, slide off the PCIe card filler plate, as needed, and carefully install the PCIe card.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The card must be fully and evenly seated in the slot.

6. Repeat the preceding step for the remaining PCIe cards that you set aside.

7. Close the side panel and tighten the thumbscrew.

Step 6: Move a caching module

You must move the caching modules from the impaired controller modules to the replacement controller module when replacing a controller module.

1. Locate the caching module at the rear of the controller module and remove it:
   a. Press the release tab.
   b. Remove the heatsink.

      The storage system comes with two slots available for the caching module and only one slot is occupied, by default.

2. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.
3. Verify that the caching module is seated squarely and completely in the socket. If necessary, remove the caching module and reseat it into the socket.
4. Reseat and push the heatsink down to engage the locking button on the caching module housing.
5. Repeat the steps if you have a second caching module. Close the controller module cover.

Step 7: Install the controller

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the CPU air duct.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:

If your system is in…	Then perform these steps…
An HA pair	`The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.` a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors. The controller begins to boot as soon as it is seated in the chassis. 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. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. Select the option to boot to Maintenance mode from the displayed menu.

If your system is in…	Then perform these steps…
A stand-alone configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. ⓘ 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, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message. ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode. e. From the boot menu, select the option for Maintenance mode.

Important: During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

Restore and verify the system configuration - FAS8200

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device..
   - cna is a Converged Network Adapter or interface not connected to a network or storage device.
   - fcal is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - mem is system memory.
   - nic is a network interface card.
   - `nvram` is nonvolatile RAM.
   - `nvmem` is a hybrid of NVRAM and system memory.
   - `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev dev_name` *dev_name* can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev dev_name` After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev dev_name -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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` -selection only disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the controller: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The system displays the LOADER prompt. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Recable the system and reassign disks - FAS8200

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must use the correct procedure for your configuration.

Option 1: Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch. `boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
--------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for `savecore` command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the `savecore` command: `system node run -node *local-node-name* partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode *replacement_node_name*`

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

> If the giveback is vetoed, you can consider overriding the vetoes.

Find the High-Availability Configuration content for your version of ONTAP 9

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

Option 2: Manually reassign the system ID on systems in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering `Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid`,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

   ```
   dr-group-id cluster         node                 node-systemid dr-
   partner-systemid
    ----------- --------------------- -------------------- -------------
   -------------------
    1           Cluster_A             Node_A_1             536872914
   118073209
    1           Cluster_B             Node_B_1             118073209
   536872914
    2 entries were displayed.
   ```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

   ```
   Local System ID: 118065481
       ...
       ...
   ```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                 POOL   SERIAL NUMBER  HOME
-------    -------------         -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Verify that the coredumps are saved: `system node run -node` *`local-node-name`* `partner savecore`

      If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node` *`local-node-name`* `partner savecore -s command`.</info>.

   c. Return to the admin privilege level: `set -privilege admin`
7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

       You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).
    b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`
    c. Return to the admin privilege level: `set -privilege admin`

Complete system restoration - FAS8200

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My

Support section under Software licenses.

> The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and register the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - FAS8200

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes

that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

1. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

2. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
3. Unplug the battery:

   > The NVMEM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after Data ONTAP has successfully booted.

     a. Open the CPU air duct and locate the NVMEM battery.

1	NVMEM battery lock tab
2	NVMEM battery

b. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.

c. Wait a few seconds, and then plug the battery back into the socket.

4. Check the NVMEM LED on the controller module.
5. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

6. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
7. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:

8. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

9. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

10. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

11. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

12. Close the controller module cover.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

3. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.

b. After the controller boots to Maintenance mode, halt the controller: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

- A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	**Then…**
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.

If your controller is in…	Then…
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6 (Two-node MetroCluster only): Switch back aggregates

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a fan - FAS8200

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press down the release latch on the fan module cam handle, and then pull the cam handle downward.

   The fan module moves a little bit away from the chassis.

1	Cam handle

❷	Fan module
❸	Cam handle release latch
❹	Fan module Attention LED

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVMEM battery - FAS8200

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*>`

```
system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

❶	Thumbscrew
❷	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

     The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

     - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
     - If the LED is on and power is on, unwritten data is stored on NVMEM.

       This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Open the CPU air duct and locate the NVMEM battery.

1	Battery lock tab
2	NVMEM battery pack

3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Remove the replacement battery from its package.
5. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.
6. Close the CPU air duct.

   Make sure that the plug locks down to the socket.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

3. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: SLDIAG: No log messages are present. c. Exit Maintenance mode: `halt` The controller displays the LOADER prompt. d. Boot the controller from the LOADER prompt: `bye` e. Return the controller to normal operation:

If your controller is in…	**Then…**
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If your controller is in…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe card - FAS8200

To replace a PCIe card, you must perform a specific sequence of tasks.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace a PCIe card

To replace a PCIe card, locate it within the controller and follow the specific sequence of steps.

1. Loosen the thumbscrew on the controller module side panel.
2. Swing the side panel off the controller module.

1	Side panel
2	PCIe card

3. Remove the PCIe card from the controller module and set it aside.
4. Install the replacement PCIe card.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The PCIe card must be fully and evenly seated in the slot.

   > If you are installing a card in the bottom slot and cannot see the card socket well, remove the top card so that you can see the card socket, install the card, and then reinstall the card you removed from the top slot.

5. Close the side panel and tighten the thumbscrew.

Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

3. Complete the reinstallation of the controller module:

   The controller module begins to boot as soon as it is fully seated in the chassis.

If your system is in…	Then perform these steps…
An HA pair	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. > 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. If you have not already done so, reconnect the cables to the controller module. d. Bind the cables to the cable management device with the hook and loop strap.
A two-node MetroCluster configuration	a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module. > 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. If you have not already done so, reconnect the cables to the controller module. d. Bind the cables to the cable management device with the hook and loop strap. e. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.

4. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the nicadmin convert command from Maintenance mode.

> Be sure to exit Maintenance mode after completing the conversion.

5. Return the controller to normal operation:

If your system is in…	Issue this command from the partner's console…
An HA pair	`storage failover giveback -ofnode` *`impaired_node_name`*
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.

6. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5 (two-node MetroCluster only): Switch back aggregate

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - FAS8200

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.

3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Press down the release latch on the power supply cam handle, and then lower the cam handle to the fully open position to release the power supply from the mid plane.

1	Power supply

❷	Cam handle release latch
❸	Power and Fault LEDs
❹	Cam handle
❺	Power cable locking mechanism

5. Use the cam handle to slide the power supply out of the system.

   When removing a power supply, always use two hands to support its weight.

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

   The power supplies are keyed and can only be installed one way.

   Do not use excessive force when sliding the power supply into the system. You can damage the connector.

8. Push firmly on the power supply cam handle to seat it all the way into the chassis, and then push the cam handle to the closed position, making sure that the cam handle release latch clicks into its locked position.
9. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

1. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

   The power supply LEDs are lit when the power supply comes online.

2. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - FAS8200

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system

- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Open the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

4. Loosen the thumbscrew on the cam handle on the controller module.

1	Thumbscrew
2	Cam handle

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Step 3: Replace the RTC Battery

To replace the RTC battery, locate them inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

Step 4: Reinstall the controller module and setting time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

1. If you have not already done so, close the air duct or controller module cover.

2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Tighten the thumbscrew on the cam handle on back of the controller module.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

FAS8300 and FAS8700 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

Quick guide - FAS8300 and FAS8700

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

FAS8300 and FAS8700 Installation and Setup Instructions

Videos - FAS8300 and FAS8700

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

FAS8300 and FAS8700 Installation and setup instructions

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - FAS8300 and FAS8700

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Step 1: Prepare for installation

To install your system, you need to create an account, register the system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
100 GbE cable (QSF(28)	X66211A-05 (112-00595), 0.5m X66211A-1 (112-00573), 1m X66211A-2 (112-00574), 2m X66211A-5 (112-00574), 5m		Storage, cluster interconnect/HA, and Ethernet data (order-dependent)
25 GbE cable (SFP28s)	X66240-2 (112-00598), 2m X66240-5 (112-00639), 5m		GbE network connection (order-dependent)
32 Gb FC (SFP+ Op)	X66250-2 (112-00342), 2m X66250-5 (112-00344), 5m X66250-15 (112-00346), 15m		FC network connection
Storage Cables	X66030A (112-00435), .5m X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		mini-SAS HD to mini-SAS HD cables (order-dependent)
Optical cables	X66250-2-N-C (112-00342)		16 Gb FC or 25GbE cables for mezzanine cards (order-dependent)
RJ-45 (order dependent)	X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network
Micro-USB console cable	Not applicable		Console connection used during software setup if laptop or console does not support network discovery.
Power cables	Not applicable		Powering up the system

4. Review the *NetApp ONTAP Confiuration Guide* and collect the required information listed in that guide.

   ONTAP Configuration Guide

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.

3. Attach cable management devices (as shown).

4. Place the bezel on the front of the system.

Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Cable a two-node switchless cluster

The optional data ports, optional NIC cards, and management ports on the controller modules are connected to switches. The cluster interconnect and HA ports are cabled on both controller modules.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Two-node switchless cluster cabling

2. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Option 2: Cable a switched cluster

The optional data ports, optional NIC cards, mezzanine cards, and management ports on the controller modules are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Switched cluster cabling

2. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Step 4: Cable controllers to drive shelves

Option 1: Cable the controllers to SAS drive shelves

You must cable each controller to the IOM modules on both SAS drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the DS224-C are down.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustration to cable your controllers to two drive shelves.

   Cabling the controllers to SAS drive shelves

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

4. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

5. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

      XXXXX is the system serial number for the target node.

   System Manager opens.

6. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

   ONTAP Configuration Guide

7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

b. Register your system.

NetApp Product Registration

c. Download Active IQ Config Advisor.

NetApp Downloads: Config Advisor

8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

   See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet .
   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   FAS8300 and FAS8700 shown.

   Power on the controllers

   Initial booting may take up to eight minutes.

4. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.

If the management network has DHCP…	Then…
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

5. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

6. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

7. Verify the health of your system by running Config Advisor.
8. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF FAS8300 and FAS8700

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys - AFF fas8300 and FAS8700

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

   > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. You can safely shut down the controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager external sync`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
     c. You can safely shut down the controller.
  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

        Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

        mysupport.netapp.com

     b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
     c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
     d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
     f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     g. Return to admin mode: `set -priv admin`
     h. You can safely shut down the controller.

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*>`

```
system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node Metrocluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the boot media - FAS8300 and FAS8700

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

1	Locking latches
2	Slide controller out of chassis

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 2: Replace the boot media

You must locate the boot media in the controller module (see the FRU map on the controller module), and then follow the directions to replace it.

Before you begin

Although the contents of the boot media is encrypted, it is a best practice to erase the contents of the boot media before replacing it. For more information, see the Statement of Volatility for your system on the NetApp Support Site.

> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustrations, or the written steps to replace the boot media.

Replacing the boot media

Steps

1. Open the air duct:

1	Locking tabs
2	Slide air duct toward back of controller
3	Rotate air duct up

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

2. Locate and remove the boot media from the controller module:

1	Press blue button
2	Rotate boot media up and remove from socket

   a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
   b. Rotate the boot media up and gently pull the boot media out of the socket.
3. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Placing a finger at the end of the boot media by the blue button, push down on the boot media end to engage the blue locking button.
   c. While pushing down on the boot media, lift the blue locking button to lock the boot media in place.
6. Close the air duct.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed does not have a boot image, so you need to transfer a boot image using a USB flash drive.

Before you begin

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the `var` file system.

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
   a. Download the service image to your work space on your laptop.
   b. Unzip the service image.

      > If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

      There are two folders in the unzipped service image file:

      - `boot`
      - `efi`

   c. Copy the `efi` folder to the top directory on the USB flash drive.

      The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

   d. Remove the USB flash drive from your laptop.
2. If you have not already done so, close the air duct.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
4. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs or QSFPs) if they were removed.
5. Plug the power cable into the power supply and reinstall the power cable retainer.
6. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

7. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. If you have not already done so, reinstall the cable management device.
8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then `halt` the controller to boot to LOADER.

9. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:
   a. Boot to Maintenance mode: `boot_ontap maint`
   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t` *`initiator adapter_name`*
   c. Halt to return to Maintenance mode: `halt`

The changes will be implemented when the system is booted.

Boot the recovery image - AFF FAS8300 and FAS8700

The procedure for booting the impaired controller from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1: Most systems

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.

3. Restore the `var` file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy controller to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the controller to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the controller.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
   - If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.
6. From the LOADER prompt, enter the `boot_ontap` command.

*If you see…	Then…*
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner controller.
8. Give back the controller using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Controller is in a two-node MetroCluster

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. After the image is installed, start the restoration process:
   a. Press `n` when prompted to restore the backup configuration.
   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
   e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF fas8300 and FAS8700

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the

configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - AFF fas8300 and FAS8700

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.

6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


   ```
   ---------------------------BEGIN BACKUP---------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   ---------------------------END BACKUP---------------------------
   ```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show`

and `storage failover show-giveback` commands.

Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.

Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF fas8300 and FAS8700

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module - FAS8300 and FAS8700

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

- You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this tasks

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller.

ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

Steps

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run -node node_name -device-id device_id`
   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

The output should display the caching module status as erased.

2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=_number_of_hours_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
4. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y`.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace a caching module

To replace a caching module, referred to as the Flash Cache on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps. See the FRU map on the controller module for the location of the Flash Cache.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- Although the contents of the caching module is encrypted, it is a best practice to erase the contents of the module before replacing it. For more information, see the Statement of Volatility for your system on the NetApp Support Site.

  > You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

- All other components in the storage system must be functioning properly; if not, you must contact technical support.

You can use the following animation, illustration, or the written steps to replace a caching module.

Replacing the caching module

Steps

1. If you are not already grounded, properly ground yourself.
2. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
3. Using the FRU map on the controller module, locate the failed caching module and remove it:

   Depending on your configuration, there may be zero, one, or two caching modules in the controller module. The failed caching module's LED is lit.

   a. Press the blue release tab.

      The caching module end rises clear of the release tab.

   b. Rotate the caching module up and slide it out of the socket.
4. Install the replacement caching module:
   a. Align the edges of the replacement caching module with the socket and gently insert it into the socket.
   b. Rotate the caching module downward toward the motherboard.
   c. Placing your finger at the end of the caching module by the blue button, firmly push down on the caching module end, and then lift the locking button to lock the caching module in place.
5. Close the air duct:
   a. Rotate the air duct down to the controller module.
   b. Slide the air duct toward the risers to lock it in place.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

Steps

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so

that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Stress-Test system** from the displayed menu.
5. Select **M.2 NVME Drive Stress** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

Steps

1. Recable the system, as needed.

If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Complete the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - FAS8300 and FAS8700

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is disruptive. For a two-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - FAS8300 and FAS8700

Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

Answer `y` when prompted.

Option 2: Controller is in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Move and replace hardware - FAS8300 and FAS8700

Move the fans, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or

system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

To replace the chassis, you must remove the controller modules from the old chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move the fans

To move the fan modules to the replacement chassis when replacing the chassis, you must perform a specific sequence of tasks.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

4. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   > The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

5. Set the fan module aside.
6. Repeat the preceding steps for any remaining fan modules.
7. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.

8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Repeat these steps for the remaining fan modules.

Step 3: Replace a chassis from within the equipment rack or system cabinet

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

Steps

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or equipment rack.
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. If you have not already done so, install the bezel.

Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run the diagnostic test.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.
3. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

   > If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

4. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - FAS8300 and FAS8700

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:

   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for HA-state can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Complete the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller

Overview of controller module replacement - FAS8300 and FAS8700

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

  If this is the procedure you should use, note that the controller replacement procedure for a controller in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement node* is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - FAS8300 and FAS8700

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=_number_of_hours_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module..
Waiting for giveback…	Press Ctrl-C, and then respond `y`.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the controller module hardware - FAS8300 and FAS8700

To replace the controller module hardware, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.
8. On the replacement controller module, open the air duct and remove the empty risers from the controller module using the animation, illustration, or the written steps:

   Removing the empty risers from the replacement controller module

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
c. Rotate the riser locking latch on the left side of riser 1 up and toward air duct, lift the riser up, and then set it aside.
d. Repeat the previous step for the remaining risers.

Step 2: Move the power supplies

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

You can use the following animation, illustration, or the written steps to move the power supplies to the replacement controller module.

Moving the power supplies

1. Remove the power supply:
   a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
   b. Press the blue locking tab to release the power supply from the chassis.
   c. Using both hands, pull the power supply out of the chassis, and then set it aside.
2. Move the power supply to the new controller module, and then install it.
3. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

4. Repeat the preceding steps for any remaining power supplies.

Step 3: Move the NVDIMM battery

To move the NVDIMM battery from the impaired controller module to the replacement controller module, you must perform a specific sequence of steps.

You can use the following animation, illustration, or the written steps to move the NVDIMM battery from the impaired controller module to the replacement controller module.

Moving the NVDIMM battery

1. Open the air duct:

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

2. Locate the NVDIMM battery in the controller module.

1. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
2. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
3. Move the battery to the replacement controller module.
4. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.

> Do not plug the battery cable back into the motherboard until instructed to do so.

Step 4: Move the boot media

You must locate the boot media, and then follow the directions to remove it from the impaired controller module and insert it into the replacement controller module.

You can use the following animation, illustration, or the written steps to move the boot media from the impaired

controller module to the replacement controller module.

Moving the boot media

1. Locate and remove the boot media from the controller module:
   a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
   b. Rotate the boot media up and gently pull the boot media out of the socket.
2. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
3. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

4. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Press the blue locking button so that it is in the open position.
   c. Placing your fingers at the end of the boot media by the blue button, firmly push down on the boot media end to engage the blue locking button.

Step 5: Move the PCIe risers and mezzanine card

As part of the controller replacement process, you must move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

You can use the following animations, illustrations. or the written steps to move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

Moving PCIe riser 1 and 2 (left and middle risers):

Moving PCI risers 1 and 2

Moving the mezzanine card and riser 3 (right riser):

Moving the mezzanine card and riser 3

1. Move PCIe risers one and two from the impaired controller module to the replacement controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, and then move it to the replacement controller module.
   d. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins, push the riser squarely into the socket on the motherboard, and then rotate the latch down flush with the sheet metal on the riser.
   e. Repeat this step for riser number 2.
2. Remove riser number 3, remove the mezzanine card, and install both into the replacement controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, and then set it aside on a stable, flat surface.
   d. Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket, and then move it to the replacement controller module.

e. Install the mezzanine in the replacement controller and secure it with the thumbscrews.

f. Install the third riser in the replacement controller module.

Step 6: Move caching modules

You must move the caching modules from the impaired controller modules to the replacement controller module when replacing a controller module.

You can use the following animation, illustration, or the written steps to move caching modules to the new controller module.

Moving the caching modules

1. If you are not already grounded, properly ground yourself.
2. Move the caching modules from the impaired controller module to the replacement controller module:
   a. Press the blue release tab at the end of the caching module, rotate the module up, and then remove the module from the socket.
   b. Move the caching module to the same socket on the replacement controller module.
   c. Align the edges of the caching module with the socket and gently insert the module as far into the socket as it will go.
   d. Rotate the caching module downward toward the motherboard.

e. Placing your finger at the end of the caching module by the blue button, firmly push down on the caching module end, and then lift the locking button to lock the caching module in place.

Step 7: Move the DIMMs

You need to locate the DIMMs, and then move them from the impaired controller module to the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

You can use the following animation, illustration, or the written steps to move the DIMMs from the impaired controller module to the replacement controller module.

Moving the DIMMs

1. Locate the DIMMs on your controller module.

2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Verify that the NVDIMM battery is not plugged into the new controller module.
4. Move the DIMMs from the impaired controller module to the replacement controller module:

   > Make sure that you install the each DIMM into the same slot it occupied in the impaired controller module.

   a. Eject the DIMM from its slot by slowly pushing apart the DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

      > Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

   b. Locate the corresponding DIMM slot on the replacement controller module.
   c. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

      The DIMMs fit tightly in the socket, but should go in easily. If not, realign the DIMM with the socket and reinsert it.

   d. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
   e. Repeat these substeps for the remaining DIMMs.
5. Plug the NVDIMM battery into the motherboard.

   Make sure that the plug locks down onto the controller module.

Step 8: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the replacement controller module in the chassis.

Installing the controller module

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

Restore and verify the system configuration - FAS8300 and FAS8700

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for `HA-state` can be one of the following:

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select `Reboot` from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

You must complete a series of tasks before restoring your system to full operation.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.

You must use the correct procedure for your configuration:

Controller redundancy	Then use this procedure…
HA pair	Option 1: Verify the system ID change on an HA system]
Two-node MetroCluster configuration	Option 2: Manually reassign the system ID on systems in a two-node MetroCluster configuration

Option 1: Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system node run -node` *`local-node-name`* `partner savecore -s`

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

      The *replacement* controller takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration Guide for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* controller should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

Option 2: Manually reassign the system ID on systems in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering `Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid`,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

```
dr-group-id cluster         node                 node-systemid dr-
partner-systemid
 ----------- --------------------- -------------------- -------------
-------------------
 1           Cluster_A             Node_A_1             536872914
118073209
 1           Cluster_B             Node_B_1             118073209
536872914
 2 entries were displayed.
```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

```
Local System ID: 118065481
    ...
    ...
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                 POOL   SERIAL NUMBER  HOME
-------    -------------         -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:

a. Change to the advanced privilege level: `set -privilege advanced`

   You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

b. Verify that the coredumps are saved: `system node run -node local-node-name partner savecore`

   If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node local-node-name partner savecore -s command`.</info>.

c. Return to the admin privilege level: `set -privilege admin`

7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`

c. Return to the admin privilege level: `set -privilege admin`

Complete system restoration - FAS8300 and FAS8700

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption

functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verify LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a DIMM - FAS8300 and FAS8700

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.

If the impaired controller is displaying…	Then…
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace system DIMMs

Replacing a system DIMM involves identifying the target DIMM through the associated error message, locating the target DIMM using the FRU map on the air duct or the lit LED on the motherboard, and then replacing the DIMM.

You can use the following animation, illustration, or the written steps to replace a system DIMM.

> The animation and illustration shows empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Replacing a system DIMM

The number and location of DIMMS in your system depends on the model of your system. Refer to FRU map on the air duct for more information.

- If you have a FAS8300 system, the system DIMMs are located in sockets 2, 4, 13, and 15.

- If you have a FAS8700 system, the system DIMMs are located in slots 2, 4, 7, 9, 13, 15, 18, and 20.
- The NVDIMM is located in slot 11.

Steps

1. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
4. Eject the DIMM from its socket by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the socket.

   > Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
8. Close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, drawing, or the written steps to install the controller module in the chassis.

Installing the controller module

Steps

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced a system DIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Select an option from the displayed sub-menu and run the test.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select `Reboot` from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

Steps

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a fan module - FAS8300 and FAS8700

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

You can use the following animation, illustration, or the written steps to hot-swap a fan module.

Replacing a fan

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   > The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The Attention LED should not be lit after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
11. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an NVDIMM - FAS8300 and FAS8700

You must replace the NVDIMM in the controller module when your system registers that the flash lifetime is almost at an end or that the identified NVDIMM is not healthy in general; failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following , illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace the NVDIMM

To replace the NVDIMM, you must locate it in the controller module using the FRU map on top of the air duct or locate the Attention LED using the FRU Map on the top of the slot 1 riser.

- The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.
- Although the contents of the NVDIMM is encrypted, it is a best practice to erase the contents of the NVDIMM before replacing it. For more information, see the Statement of Volatility on the NetApp Support Site.

> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the NVDIMM.

> The animation and illustration show empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Replacing the NVDIMM

Steps

1. Open the air duct and then locate the NVDIMM in slot 11 on your controller module.

   The NVDIMM looks significantly different than system DIMMs.

2. Eject the NVDIMM from its slot by slowly pushing apart the two NVDIMM ejector tabs on either side of the NVDIMM, and then slide the NVDIMM out of the socket and set it aside.

   Carefully hold the NVDIMM by the edges to avoid pressure on the components on the NVDIMM circuit board.

3. Remove the replacement NVDIMM from the antistatic shipping bag, hold the NVDIMM by the corners, and then align it to the slot.

   The notch among the pins on the NVDIMM should line up with the tab in the socket.

4. Locate the slot where you are installing the NVDIMM.
5. Insert the NVDIMM squarely into the slot.

   The NVDIMM fits tightly in the slot, but should go in easily. If not, realign the NVDIMM with the slot and reinsert it.

   > Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
7. Close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

Steps

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

> You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.
   g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced the NVDIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.

5. Select **NVDIMM Test** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select `Reboot` from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

Steps

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` `impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVDIMM battery - FAS8300 and FAS8700

To replace the NVDIMM battery, you must remove the controller module, remove the battery, replace the battery, and then reinstall the controller module.

All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace the NVDIMM battery

To replace the NVDIMM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module. See the FRU map

inside the controller module to locate the NVDIMM battery.

The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.

You can use the following animation, illustration, or the written steps to replace the NVDIMM battery.

Replacing the NVDIMM battery

Steps

1. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
2. Locate the NVDIMM battery in the controller module.
3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Remove the replacement battery from its package.
6. Align the battery module with the opening for the battery, and then gently push the battery into slot until it

locks into place.

7. Plug the battery plug back into the controller module, and then close the air duct.

Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

Steps

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   You will connect the rest of the cables to the controller module later in this procedure.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

   > If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

All commands in the diagnostic procedures are issued from the controller where the component is being replaced.

Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select `Reboot` from the menu to reboot the system.

Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

Steps

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 7: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a PCIe or mezzanine card - FAS8300 and FAS8700

To replace a PCIe or mezzanine card, you must disconnect the cables and any SFP and QSFP modules from the cards, replace the failed PCIe or mezzanine card, and then recable the cards.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.

2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace a PCIe card

To replace a PCIe card, you must locate the failed PCIe card, remove the riser that contains the card from the controller module, replace the card, and then reinstall the PCIe riser in the controller module.

You can use the following animation, illustration, or the written steps to replace a PCIe card.

Replacing a PCIe card

Steps

1. Remove the riser containing the card to be replaced:
   a. Open the air duct by pressing the locking tabs on the sides of the air duct, slide it toward the back of the controller module, and then rotate it to its completely open position.
   b. Remove any SFP or QSFP modules that might be in the PCIe cards.
   c. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   d. Lift the riser up straight up and set it aside on a stable flat surface,
2. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. For risers 2 and 3 only, swing the side panel up.
   d. Remove the PCIe card from the riser by gently pushing up on the bracket and lift the card straight out of the socket.
3. Install the replacement PCIe card in the riser by aligning the card with the socket, press the card into the socket and then close the side panel on the riser, if present.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The PCIe card must be fully and evenly seated in the slot.

   > If you are installing a card in the bottom slot and cannot see the card socket well, remove the top card so that you can see the card socket, install the card, and then reinstall the card you removed from the top slot.

4. Reinstall the riser:
   a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.
   b. Push the riser squarely into the socket on the motherboard.
   c. Rotate the latch down flush with the sheet metal on the riser.

Step 4: Replace the mezzanine card

The mezzanine card is located under riser number 3 (slots 4 and 5). You must remove that riser to access the mezzanine card, replace the mezzanine card, and then reinstall riser number 3. See the FRU map on the controller module for more information.

You can use the following animation, illustration, or the written steps to replace the mezzanine card.

Replacing the mezzanine card

Steps

1. Remove riser number 3 (slots 4 and 5):
   a. Open the air duct by pressing the locking tabs on the sides of the air duct, slide it toward the back of the controller module, and then rotate it to its completely open position.
   b. Remove any SFP or QSFP modules that might be in the PCIe cards.
   c. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   d. Lift the riser up, and then set it aside on a stable, flat surface.
2. Replace the mezzanine card:
   a. Remove any QSFP or SFP modules from the card.
   b. Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket and set it aside.
   c. Align the replacement mezzanine card over the socket and the guide pins and gently push the card into the socket.
   d. Tighten the thumbscrews on the mezzanine card.
3. Reinstall the riser:
   a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.

b. Push the riser squarely into the socket on the motherboard.

c. Rotate the latch down flush with the sheet metal on the riser.

Step 5: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

Steps

1. If you have not already done so, close the air duct.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. Complete the installation of the controller module:

   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.

   b. Using the locking latches, firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.

5. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

6. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

Steps

1. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 8: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a power supply - FAS8300 and FAS8700

Replacing a power supply (PSU) involves disconnecting the target PSU from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting the replacement PSU to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

You can use the following animation, illustration, or the written steps to replace the power supply.

Replacing a power supply

Steps

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Remove the power supply:
   a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
   b. Press the blue locking tab to release the power supply from the chassis.
   c. Using both hands, pull the power supply out of the chassis, and then set it aside.
5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Rotate the cam handle so that it is flush against the power supply.
7. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.

b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

8. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery - FAS8300 and FAS8700

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Place the controller module on a stable, flat surface.

Step 3: Replace the RTC battery

You need to locate the RTC battery inside the controller module, and then follow the specific sequence of steps. See the FRU map inside the controller module for the location

of the RTC battery.

You can use the following animation, illustration, or the written steps to replace the RTC battery.

Replacing the RTC battery

Steps

1. If you are not already grounded, properly ground yourself.
2. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
3. Locate, remove, and then replace the RTC battery:
   a. Using the FRU map, locate the RTC battery on the controller module.
   b. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

c. Remove the replacement battery from the antistatic shipping bag.

d. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.

4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
5. Close the air duct.

Step 4: Reinstall the controller module and sett time/date after RTC battery replacement

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module

Steps

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the installation of the controller module:

a. Using the locking latches, firmly push the controller module into the chassis until it meets the midplane and is fully seated.

   The locking latches rise when the controller module is fully seated.

   > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

b. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

c. If you have not already done so, reinstall the cable management device.

d. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

   > If your system stops at the boot menu, select the option to boot to LOADER.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy controller with the `show date` command.

   b. At the LOADER prompt on the target controller, check the time and date.

   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.

   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.

   e. Confirm the date and time on the target controller.

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.

8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

FAS9000 System Documentation

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

Quick steps - AFF A700 and FAS9000

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A700 Installation and Setup Instructions

FAS9000 Installation and Setup Instructions

Video steps - AFF A700 and FAS9000

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and setup of an AFF A700 or FAS9000

Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

Detailed guide - AFF A700 and FAS9000

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

Step 1: Prepare for installation

To install your system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

Before you begin

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

Steps

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

Type of cable…	Part number and length	Connector type	For…
10 GbE network cable	X6566B-2-R6, (112-00299), 2m X6566B-3-R6, 112-00300, 3m X6566B-5-R6 , 112-00301, 5m		Network cable
40 GbE network cable 40 GbE cluster interconnect	X66100-1,112-00542, 1m X66100-3,112-00543, 3m		40 GbE network Cluster interconnect
100 GbE network cable 100 GbE storage cable	X66211A-05 (112-00595), 0.5m X66211A-1 (112-00573), 1m X66211A-2 (112-00574), 2m X66211A-5 (112-00574), 5m		Network cable Storage cable This cable applies to AFF A700 only.
Optical network cables (order dependent)	X6553-R6 (112-00188), 2m X6536-R6 (112-00090), 5m		FC host network
Cat 6, RJ-45 (order dependent)	Part numbers X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network and Ethernet data
Storage	X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		Storage
Micro-USB console cable	Not applicable		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	Not applicable		Powering up the system

4. Review the *NetApp ONTAP Confiuration Guide* and collect the required information listed in that guide.

   ONTAP Configuration Guide

Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

Steps

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

You need to be aware of the safety concerns associated with the weight of the system.

The label on the left indicates an empty chassis, while the label on the right indicates a fully-populated system.

1. Attach cable management devices (as shown).

2. Place the bezel on the front of the system.

Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

Option 1: Two-node switchless cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Cabling a two-node switchless cluster

1. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Option 2: Switched cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Switched cluster cabling

1. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

Step 4: Cable controllers to drive shelves

You can cable your new system to DS212C, DS224C, or NS224 shelves, depending on if it is an AFF or FAS system.

Option 1: Cable the controllers to DS212C or DS224C drive shelves

You must cable the shelf-to-shelf connections, and then cable both controllers to the DS212C or DS224C drive shelves.

The cables are inserted into the drive shelf with the pull-tabs facing down, while the other end of the cable is inserted into the controller storage modules with the pull-tabs up.

Steps

1. Use the following animations or illustrations to cable your drive shelves to your controllers.

> The examples use DS224C shelves. Cabling is similar with other supported SAS drive shelves.

   - Cabling SAS shelves in FAS9000, AFF A700, and ASA AFF A700, ONTAP 9.7 and earlier:

   Cabling SAS storage - ONTAP 9.7 and earlier

- Cabling SAS shelves in FAS9000, AFF A700, and ASA AFF A700, ONTAP 9.8 and later:

Cabling SAS storage - ONTAP 9.8 and later

If you have more than one drive shelf stack, see the *Installation and Cabling Guide* for your drive shelf type.

Install and cable shelves for a new system installation - shelves with IOM12 modules

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Option 2: Cable the controllers to a single NS224 drive shelf in AFF A700 and ASA AFF A700 systems running ONTAP 9.8 and later only

You must cable each controller to the NSM modules on the NS224 drive shelf on an AFF A700 or ASA AFF A700 running system ONTAP 9.8 or later.

- This task applies to AFF A700 and ASA AFF A700 running ONTAP 9.8 or later only.

- The systems must have at least one X91148A module installed in slots 3 and/or 7 for each controller. The animation or illustrations show this module installed in both slots 3 and 7.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustrations to cable your controllers with two X91148A storage modules to a single NS224 drive shelf, or use the diagram to cable your controllers with one X91148A storage module to a single NS224 drive shelf.

   Cabling a single NS224 shelf - ONTAP 9.8 and later

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Option 3: Cable the controllers to two NS224 drive shelves in AFF A700 and ASA AFF A700 systems running ONTAP 9.8 and later only

You must cable each controller to the NSM modules on the NS224 drive shelves on an AFF A700 or ASA AFF A700 running system ONTAP 9.8 or later.

- This task applies to AFF A700 and ASA AFF A700 running ONTAP 9.8 or later only.
- The systems must have two X91148A modules, per controller, installed in slots 3 and 7.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the following animation or illustrations to cable your controllers to two NS224 drive shelves.

   Cabling two NS224 shelves - ONTAP 9.8 and later

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

Steps

1. Use the following animation to set one or more drive shelf IDs:

   If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

   Setting SAS or NVMe drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

   Turn on the power to the controllers

   > Initial booting may take up to eight minutes.

4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:

   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

      > XXXXX is the system serial number for the target node.

   System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the *NetApp*

ONTAP Configuration Guide.

ONTAP Configuration Guide

8. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

9. Verify the health of your system by running Config Advisor.
10. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Option 2: Completing system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

Steps

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet .

   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

Setting SAS or NVMe drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

   Turn on the power to the controllers

   > Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

If the management network has DHCP…	Then…
Configured	Record the IP address assigned to the new controllers.
Not configured	a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. > Check your laptop or console's online help if you do not know how to configure PuTTY. b. Enter the management IP address when prompted by the script.

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      > The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

8. Verify the health of your system by running Config Advisor.

9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

Maintain

Boot media

Overview of boot media replacement - AFF A700 and FAS9000

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz`.

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair does not require connection to a network to restore the `var` file system. The HA pair in a single chassis has an internal e0S connection, which is used to transfer `var` config between them.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

Check onboard encryption keys

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.

2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <Ino-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <Ino-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <Ino-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired node is part of an HA configuration, disable automatic giveback from the healthy node: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled,

you need to complete some other additional steps.

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

   c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

Verify NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.
   b. If the `Restored` column displays anything other than `yes`:
      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

> Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

- Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shut down the controller.

Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

b. Enter the command to display the key management information: `security key-manager onboard show-backup`

c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

Shut down the impaired controller - AFF A700 and FAS9000

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays…	Then…
The LOADER prompt	Go to Remove controller module.
`Waiting for giveback…`	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

1. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.

   This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.
NOTE: Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	**Then…**
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - AFF A700 and FAS9000

To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

1	Controller module cover locking button

Step 2: Replace the boot media

Locate the boot media using the following illustration or the FRU map on the controller module:

❶	Press release tab
❷	Boot media

1. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

   > Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

2. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
3. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

4. Push the boot media down to engage the locking button on the boot media housing.
5. Reinstall the controller module lid by aligning the pins on the lid with the slots on the motherboard carrier, and then slide the lid into place.

Step 3: Transfer the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the `var` file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the `var` file system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Recable the controller module, as needed.
3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, and then push the cam

handle to the closed position.

The node begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort….

   If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the node to boot to LOADER.

6. Set your network connection type at the LOADER prompt:

   - If you are configuring DHCP: `ifconfig e0a -auto`

     > The target port you configure is the target port you use to communicate with the impaired node from the healthy node during `var` file system restore with a network connection. You can also use the e0M port in this command.

   - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
     - filer_addr is the IP address of the storage system.
     - netmask is the network mask of the management network that is connected to the HA partner.
     - gateway is the gateway for the network.
     - dns_addr is the IP address of a name server on your network.
     - dns_domain is the Domain Name System (DNS) domain name.

       If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server's host name.

     > Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

7. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:

   a. Boot to Maintenance mode: `boot_ontap maint`
   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t` *`initiator adapter_name`*
   c. Halt to return to Maintenance mode: `halt`

   The changes will be implemented when the system is booted.

Boot the recovery image - AFF A700 and FAS9000

The procedure for booting the impaired node from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1 Boot the recovery image in most systems

You must boot the ONTAP image from the USB drive, restore the file system, and verify

the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the `var` file system:

If your system has…	Then…
A network connection	a. Press `y` when prompted to restore the backup configuration. b. Set the healthy node to advanced privilege level: `set -privilege advanced` c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Return the node to admin level: `set -privilege admin` e. Press `y` when prompted to use the restored configuration. f. Press `y` when prompted to reboot the node.
No network connection	a. Press `n` when prompted to restore the backup configuration. b. Reboot the system when prompted by the system. c. Select the **Update flash from backup config** (sync flash) option from the displayed menu. If you are prompted to continue with the update, press `y`.

If your system has…	Then…

No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:
	`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).`
	d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.
	If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:
   a. Take the node to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
   d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

*If you see…	Then…*
The login prompt	Go to the next Step.
Waiting for giveback…	a. Log into the partner node. b. Confirm the target node is ready for giveback with the `storage failover show` command.

7. Connect the console cable to the partner node.
8. Give back the node using the `storage failover giveback -fromnode local` command.
9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

   If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired node and run the `version -v` command to check the ONTAP versions.
11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Boot the recovery image in a two-node MetroCluster configuration

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. After the image is installed, start the restoration process:
   a. Press `n` when prompted to restore the backup configuration.
   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
   a. Take the node to the LOADER prompt.

b. Check the environment variable settings with the `printenv` command.

c. If an environment variable is not set as expected, modify it with the `setenv environment-variable-name changed-value` command.

d. Save your changes using the `savenv` command.

e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF A700 and FAS9000

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - AFF A700 and FAS9000

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the controller to the boot menu: `boot_ontap menu`
Waiting for giveback…	a. Enter `Ctrl-C` at the prompt b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y` c. At the LOADER prompt, enter the `boot_ontap menu` command.

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


   ```
   ---------------------------BEGIN BACKUP---------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   ---------------------------END BACKUP---------------------------
   ```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int`

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 7.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the `storage failover show` command.

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Return the failed part to NetApp - AFF A700 and FAS9000

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the caching module or add/replace a core dump module - AFF A700 and FAS9000

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation. If AutoSupport is not enabled, you can locate the failed caching module by the fault LED on the front of the module. You can also add or replace the 1TB, X9170A core dump module, which is required if you are installing NS224 drive shelves in an AFF A700 system.

Before you begin

- You must replace the failed component with a replacement FRU component you received from your provider.
- For instructions about hot swapping the caching module, see Hot-swapping a caching module.
- When removing, replacing, or adding caching or core dump modules, the target node must be halted to the LOADER.
- AFF A700 supports the 1TB core dump module, X9170A, which is required if you are adding NS224 drive shelves.
- The core dump modules can be installed in slots 6-1 and 6-2. The recommended best practice is to install the module in slot 6-1.
- The X9170A core dump module is not hot-swappable.

Step 1: Shutting down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace or add a caching module

The NVMe SSD Flash Cache modules (FlashCache or caching modules) are separate modules. They are located in the front of the NVRAM module. To replace or add a caching module, locate it on the rear of the system on slot 6, and then follow the specific sequence of steps to replace it.

Before you begin

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The target node must be at the LOADER prompt before adding or replacing the caching module.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.
3. Remove the caching module:

> If you are adding another caching module to your system, remove the blank module and go to the next step.

1	Orange release button.
2	Caching module cam handle.

a. Press the orange release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

   Be sure to support the caching module as you remove it from the NVRAM10 module.

4. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM10 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

Step 3: Add or replace an X9170A core dump module

The 1TB cache core dump, X9170A, is only used in the AFF A700 systems. The core dump module cannot be hot-swapped. The core dump module typically is located in the

front of the NVRAM module in slot 6-1 in the rear of the system. To replace or add the core dump module, locate slot 6-1, and then follow the specific sequence of steps to add or replace it.

Before you begin

- Your system must be running ONTAP 9.8 or later in order to add a core dump module.
- The X9170A core dump module is not hot-swappable.
- The target node must be at the LOADER prompt before adding or replacing the code dump module.
- You must have received two X9170 core dump modules; one for each controller.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you are replacing a failed core dump module, locate and remove it:

1	Orange release button.
2	Core dump module cam handle.

a. Locate the failed module by the amber Attention LED on the front of the module.

b. Press the orange release button on the front of the core dump module.

> Do not use the numbered and lettered I/O cam latch to eject the core dump module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the core dump module.

c. Rotate the cam handle until the core dump module begins to slide out of the NVRAM10 module.
d. Gently pull the cam handle straight toward you to remove the core dump module from the NVRAM10 module and set it aside.

   Be sure to support the core dump module as you remove it from the NVRAM10 module.

3. Install the core dump module:
   a. If you are installing a new core dump module, remove the blank module from slot 6-1.
   b. Align the edges of the core dump module with the opening in the NVRAM10 module.
   c. Gently push the core dump module into the bay until the cam handle engages.
   d. Rotate the cam handle until it locks into place.

Step 4: Reboot the controller after FRU replacement

After you replace the FRU, you must reboot the controller module.

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a caching module - AFF A700 and FAS9000

The NVMe SSD FlashCache modules (FlashCache or caching modules) are located in the front of the NVRAM10 module in Slot 6 of FAS9000 systems only. Beginning with ONTAP 9.4, you can hot-swap the caching module of the same capacity from the same or different supported vendor.

Before you begin

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.
3. Prepare the caching module slot for replacement as follows:

    a. For ONTAP 9.7 and earlier:

        i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

        ii. In admin privilege level, prepare the target NVMe slot for replacement, responding `y` when prompted whether to continue: `system controller slot module replace -node` *`node_name -slot slot_number`* The following command prepares slot 6-2 on node1 for replacement, and displays a message that it is safe to replace:

```
::> system controller slot module replace -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node node1 will be powered
off for replacement.
Do you want to continue? (y|n): `y`

The module has been successfully powered off.  It can now be
safely replaced.
After the replacement module is inserted, use the "system
controller slot module insert" command to place the module into
service.
```

iii. Display the slot status with the system controller slot module show command.

The NVMe slot status displays waiting-for-replacement in the screen output for the caching module that needs replacing.

b. For ONTAP 9.8 and later:

i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

ii. In admin privilege level, prepare the target NVMe slot for removal, responding `y` when prompted whether to continue: `system controller slot module remove -node node_name -slot slot_number` The following command prepares slot 6-2 on node1 for removal, and displays a message that it is safe to remove:

```
::> system controller slot module remove -node node1 -slot 6-2

Warning: SSD module in slot 6-2 of the node node1 will be powered
off for removal.
Do you want to continue? (y|n): `y`

The module has been successfully removed from service and powered
off. It can now be safely removed.
```

iii. Display the slot status with the `system controller slot module show` command.

The NVMe slot status displays `powered-off` in the screen output for the caching module that needs replacing.

See the Command man pages for your version of ONTAP for more details.

4. Remove the caching module:

1	Orange release button.
2	Caching module cam handle.

a. Press the orange release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

   Be sure to support the caching module as you remove it from the NVRAM10 module.

5. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM10 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

6. Bring the replacement caching module online by using the `system controller slot module insert` command as follows:

   The following command prepares slot 6-2 on node1 for power-on, and displays a message that it is

powered on:

```
::> system controller slot module insert -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node localhost will be powered
on and initialized.
Do you want to continue? (y|n): `y`

The module has been successfully powered on, initialized and placed into
service.
```

7. Verify the slot status using the `system controller slot module show` command.

   Make sure that command output reports status for slot 6-1 or 6-2 as `powered-on` and ready for operation.

8. Verify that the replacement caching module is online and recognized, and then visually confirm that the amber attention LED is not lit: `sysconfig -av slot_number`

   > If you replace the caching module with a caching module from a different vendor, the new vendor name is displayed in the command output.

9. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Chassis

Overview of chassis replacement - AFF A700 and FAS9000

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A700 and FAS9000

To replace the chassis, you must shutdown the controllers.

Option 1: Shut down the controllers

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

  The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

Steps

1. If your system has two controller modules, disable the HA pair.

If your system is running clustered ONTAP with…	Then…
Two controllers in the cluster	`cluster ha modify -configured false` `storage failover modify -node node0 -enabled false`
More than two controllers in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

Option 2: Shut down a node in a two-node MetroCluster configuration

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Move and replace hardware - AFF A700 and FAS9000

Move the fans, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the power supplies

Steps

Removing the power supplies when replacing a chassis involves turning off, disconnecting, and then removing the power supply from the old chassis.

1. If you are not already grounded, properly ground yourself.

2. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
3. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.

> ! When removing a power supply, always use two hands to support its weight.

1	Locking button

4. Repeat the preceding steps for any remaining power supplies.

Step 2: Remove the fans

To remove the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

Steps

1. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
2. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

1	Orange release button

3. Set the fan module aside.
4. Repeat the preceding steps for any remaining fan modules.

Step 3: Remove the controller module

To replace the chassis, you must remove the controller module or modules from the old chassis.

Steps

1. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
2. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

3. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

4. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 4: Remove the I/O modules

Steps

To remove I/O modules from the old chassis, including the NVRAM modules, follow the specific sequence of steps. You do not have to remove the FlashCache module from the NVRAM module when moving it to a new chassis.

1. Unplug any cabling associated with the target I/O module.

   Make sure that you label the cables so that you know where they came from.

2. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

3. Set the I/O module aside.
4. Repeat the preceding step for the remaining I/O modules in the old chassis.

Step 5: Remove the De-stage Controller Power Module

Steps

You must remove the de-stage controller power modules from the old chassis in preparation for installing the replacement chassis.

1. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.

1	DCPM module orange locking button

2. Set the DCPM module aside in a safe place and repeat this step for the remaining DCPM module.

Step 6: Replace a chassis from within the equipment rack or system cabinet

Steps

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.

   If the system is in a system cabinet, you might need to remove the rear tie-down bracket.

2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.

5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. Secure the rear of the chassis to the equipment rack or system cabinet.
8. If you are using the cable management brackets, remove them from the old chassis, and then install them on the replacement chassis.
9. If you have not already done so, install the bezel.

Step 7: Move the USB LED module to the new chassis

Steps

Once the new chassis is installed into the rack or cabinet, you must move the USB LED module from the old chassis to the new chassis.

1. Locate the USB LED module on the front of the old chassis, directly under the power supply bays.
2. Press the black locking button on the right side of the module to release the module from the chassis, and then slide it out of the old chassis.
3. Align the edges of the module with the USB LED bay at the bottom-front of the replacement chassis, and gently push the module all the way into the chassis until it clicks into place.

Step 8: Install the de-stage controller power module when replacing the chassis

Steps

Once the replacement chassis is installed into the rack or system cabinet, you must reinstall the de-stage controller power modules into it.

1. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.

   The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

2. Repeat this step for the remaining DCPM module.

Step 9: Install fans into the chassis

Steps

To install the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

1. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

   When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

2. Repeat these steps for the remaining fan modules.
3. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Step 10: Install I/O modules

Steps

To install I/O modules, including the NVRAM/FlashCache modules from the old chassis, follow the specific sequence of steps.

You must have the chassis installed so that you can install the I/O modules into the corresponding slots in the new chassis.

1. After the replacement chassis is installed in the rack or cabinet, install the I/O modules into their corresponding slots in the replacement chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage, and then push the I/O cam latch all the way up to lock the module in place.
2. Recable the I/O module, as needed.
3. Repeat the preceding step for the remaining I/O modules that you set aside.

> If the old chassis has blank I/O panels, move them to the replacement chassis at this time.

Step 11: Install the power supplies

Steps

Installing the power supplies when replacing a chassis involves installing the power supplies into the replacement chassis, and connecting to the power source.

1. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

   The power supplies are keyed and can only be installed one way.

   > Do not use excessive force when sliding the power supply into the system. You can damage the connector.

2. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

   > Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

3. Repeat the preceding steps for any remaining power supplies.

Step 12: Install the controller

Steps

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

2. Recable the console to the controller module, and then reconnect the management port.

3. Connect the power supplies to different power sources, and then turn them on.
4. With the cam handle in the open position, slide the controller module into the chassis and firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle until it clicks into the locked position.

   > Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.

   The controller module begins to boot as soon as it is fully seated in the chassis.

5. Repeat the preceding steps to install the second controller into the new chassis.
6. Boot each node to Maintenance mode:
   a. As each node starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

      > If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

   b. From the boot menu, select the option for Maintenance mode.

Complete the restoration and replacement process - AFF A700 and FAS9000

You must verify the HA state of the chassis, run diagnostics, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

You must verify the HA state of the chassis, and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
   a. Set the HA state for the chassis: `ha-config modify chassis` *`HA-state`*

      The value for `HA-state` can be one of the following:

      - `ha`
      - `mcc`
      - `mcc-2n`
      - `mccip`
      - `non-ha`

b. Confirm that the setting has changed: `ha-config show`

3. If you have not already done so, recable the rest of your system.
4. Exit Maintenance mode: `halt`

   The LOADER prompt appears.

Step 2: Running system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the node boots to Maintenance mode, halt the node: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      ⓘ During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second node if you are in an HA configuration.

   ⓘ Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the node to normal operation:
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true` `node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster              Configuration State    Mode
   --------------------    -------------------     ---------
    Local: cluster_B configured            normal
   Remote: cluster_A configured            normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Controller module

Overview of controller module replacement - AFF A700 and FAS9000

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- If your system is a FlexArray system or has a V_StorageAttach license, you must refer to the additional required steps before performing this procedure.
- If your system is in an HA pair, the healthy node must be able to take over the node that is being replaced (referred to in this procedure as the “impaired node”).
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

If this is the procedure you should use, note that the controller replacement procedure for a node in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired node to the *replacement* node so that the *replacement* node will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* node is the node that is being replaced.
  - The *replacement* node is the new node that is replacing the impaired node.
  - The *healthy* node is the surviving node.
- You must always capture the node's console output to a text file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the

`-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

To replace the controller module hardware, you must remove the impaired node, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

❶
Cam handle release button
❷
Cam handle

1. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

2. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

❶
Controller module cover locking button

Step 2: Move the boot media

You must locate the boot media and follow the directions to remove it from the old controller and insert it in the new controller.

Steps

1. Lift the black air duct at the back of the controller module and then locate the boot media using the following illustration or the FRU map on the controller module:

1	
Press release tab	
2	
Boot media	

2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

> Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

Step 3: Move the system DIMMs

To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

1	DIMM ejector tabs

❷	
DIMM	

5. Locate the slot where you are installing the DIMM.
6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

8. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
9. Repeat these steps for the remaining DIMMs.

Step 4: Install the controller

After you install the components into the controller module, you must install the controller module back into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
   e. Select the option to boot to Maintenance mode from the displayed menu.

Restore and verify the system configuration - AFF A700 and FAS9000

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

About this task

It is important that you apply the commands in the steps on the correct systems:

- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the HA partner of the *replacement* node.

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date` *`mm/dd/yyyy`*
5. If necessary, set the time in GMT on the replacement node: `set time` *`hh:mm:ss`*
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller module

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The value for HA-state can be one of the following:

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`

     a. Confirm that the setting has changed: `ha-config show`

Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - `bootmedia` is the system booting device.
   - `cna` is a Converged Network Adapter or interface not connected to a network or storage device.
   - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - `mem` is system memory.

- `nic` is a network interface card.
- `nvram` is nonvolatile RAM.
- `nvmem` is a hybrid of NVRAM and system memory.
- `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev _dev_name` `dev_name` can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` + `-selection only` disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev dev_name` After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` e. Verify that no tests failed: `sldiag device status -dev dev_name -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.

If you want to run diagnostic tests on…	Then…
Multiple components at the same time	a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently. b. List the individual tests for the device: `sldiag device show -dev dev_name` c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` `-selection only` disables all other tests that you do not want to run for the device. d. Verify that the tests were modified: `sldiag device show` e. Repeat these substeps for each device that you want to run concurrently. f. Run diagnostics on all of the devices: `sldiag device run` Do not add to or modify your entries after you start running diagnostics. After the test is complete, the following message is displayed: `*> <SLDIAG:_ALL_TESTS_COMPLETED>` g. Verify that there are no hardware problems on the node: `sldiag device status -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode: `halt` The node displays the LOADER prompt. d. Boot the node from the LOADER prompt: `bye` e. Return the node to normal operation:
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the `storage failover modify` command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Recable the system and reassign disks - AFF A700 and FAS9000

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

After running diagnostics, you must recable the controller module's storage and network connections.

Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* node and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

1. If the *replacement* node is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.`boot_ontap`
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired node, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> `storage failover show`
                                      Takeover
Node               Partner            Possible     State Description
------------       ------------       --------
-------------------------------------
node1              node2              false        System ID changed on
partner (Old:
                                                     151759755, New:
151759706), In takeover
node2              node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt

appears (*>).

b. Save any coredumps: `system node run -node local-node-name partner savecore`

c. Wait for the `savecore`command to complete before issuing the giveback.

   You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

   a. From the healthy node, give back the replaced node's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* node takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration Guide for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the System ID changed on partner message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* node should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID
Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the node: `metrocluster node show`

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each node will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the node is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a node on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* node is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each node is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each node: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A700 and FAS9000

To complete the replacement procedure and restore your system to full operation, you must recable the storage, restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller. You must complete a series of tasks before restoring your system to full operation.

Step 1: Install licenses for the replacement node in ONTAP

You must install new licenses for the *replacement* node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

If the node is in a MetroCluster configuration and all nodes at a site have been replaced, license keys must be installed on the *replacement* node or nodes prior to switchback.

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   NetApp Support

   > The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

Steps

1. Install each license key: `system license add -license-code license-key, license-key...`
2. Remove the old licenses, if desired:
   a. Check for unused licenses: `license clean-up -unused -simulate`
   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restoring Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verifying LIFs and registering the serial number

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, and register the serial number of the *replacement* node if AutoSupport is enabled, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert`

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4 (MetroCluster only): Switching back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a de-stage controller power module (DCPM) - AFF A700 and FAS9000

To hot-swap a de-stage controller power module (DCPM), which contains the NVRAM10 battery, you must locate the failed DCPM module, remove it from the chassis, and install the replacement DCPM module.

You must have a replacement DCPM module in-hand before removing the failed module from the chassis and it must be replaced within five minutes of removal. Once the DCPM module is removed from the chassis, there is no shutdown protection for the controller module that owns the DCPM module, other than failover to the other controller module.

Replacing the DCPM module

To replace the DCPM module in your system, you must remove the failed DCPM module from the system and then replace it with a new DCPM module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel on the front of the system and set it aside.
3. Locate the failed DCPM module in the front of the system by looking for the Attention LED on the module.

   The LED will be steady amber if the module is faulty.

> The DCPM module must be replaced in the chassis within five minutes of removal or the associated controller will shut down.

4. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.

1	DCPM module orange locking button

5. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.

> The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

The DCPM module LED lights when the module is fully seated into the chassis.

Dispose of batteries

You must dispose of batteries according to the local regulations regarding battery recycling or disposal. If you cannot properly dispose of batteries, you must return the batteries to NetApp, as described in the RMA instructions that are shipped with the kit.

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the

replacement procedure.

Replace a DIMM - AFF A700 and FAS9000

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller

module.

1	Controller module cover locking button

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

> Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

1	DIMM ejector tabs
2	DIMM

4. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   The notch among the pins on the DIMM should line up with the tab in the socket.

5. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   > Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
7. Close the controller module cover.

Step 4: Install the controller

After you install the components into the controller module, you must install the controller module back into the system chassis and boot the operating system.

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   > Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports only, so that you can access the system to perform the tasks in the following sections.

   > You will connect the rest of the cables to the controller module later in this procedure.

5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      > Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
   e. Select the option to boot to Maintenance mode from the displayed menu.

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.

b. After the node boots to Maintenance mode, halt the node: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

- A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy node remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

If the system-level diagnostics tests…	**Then…**
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: *SLDIAG: No log messages are present.* a. Exit Maintenance mode: `halt` The node displays the LOADER prompt. b. Boot the node from the LOADER prompt: `bye` c. Return the node to normal operation.
An HA pair	Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`* If you disabled automatic giveback, re-enable it with the storage failover modify command.

If the system-level diagnostics tests…	Then…
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem: a. Exit Maintenance mode: `halt` After you issue the command, wait until the system stops at the LOADER prompt. b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: ◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. ◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. 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. d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu: ◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. ◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on. e. Select Boot to maintenance mode from the menu. f. Exit Maintenance mode by entering the following command: `halt` After you issue the command, wait until the system stops at the LOADER prompt. g. Rerun the system-level diagnostic test.

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a fan - AFF A700 and FAS9000

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

   > The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

1	Orange release button

5. Set the fan module aside.
6. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

   When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

7. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
8. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an I/O module - AFF A700 and FAS9000

To replace an I/O module, you must perform a specific sequence of tasks.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data

from the impaired controller storage.

About this task

If you have a 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message`

`MAINT=number_of_hours_downh`

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`

If the impaired controller…	Then…
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace I/O modules

To replace an I/O module, locate it within the chassis and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug any cabling associated with the target I/O module.

   Make sure that you label the cables so that you know where they came from.

3. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

4. Set the I/O module aside.
5. Install the replacement I/O module into the chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.
6. Recable the I/O module, as needed.

Step 3: Reboot the controller after PCIe module replacement

After you replace a PCIe module, you must reboot the controller module.

Steps

1. If the node is at the LOADER prompt, boot the node, responding `y` if you see a prompt warning of a system ID mismatch and asking to override the system ID: `bye`
2. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the `nicadmin convert` command from Maintenance mode.

   Be sure to exit Maintenance mode after completing the conversion.

3. Return the node to normal operation:

If your system is in…	Issue this command from the partner's console…
An HA pair	`storage failover giveback -ofnode` *`impaired_node_name`*
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.

4. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace an LED USB module - AFF A700 and FAS9000

You can replace an LED USB module without interrupting service.

The FAS9000 or AFF A700 LED USB module provides connectivity to console ports and system status. Replacement of this module does not require tools.

Steps

1. Remove the old LED USB module:

a. With the bezel removed, locate the LED USB module at the front of the chassis, on the bottom left side.
b. Slide the latch to partially eject the module.
c. Pull the module out of the bay to disconnect it from the midplane. Do not leave the slot empty.

2. Install the new LED USB module:

a. Align the module to the bay with the notch in the corner of the module positioned near the slider latch on the chassis. The bay will prevent you from installing the module upside down.
b. Push the module into the bay until it is fully seated flush with the chassis.

   There is an audible click when the module is secure and connected to the midplane.

Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the NVRAM module or NVRAM DIMMs - AFF A700 and FAS9000

The NVRAM module consists of the NVRAM10 and DIMMs and up to two NVMe SSD Flash Cache modules (FlashCache or caching modules) per NVRAM module. You can replace a failed NVRAM module or the DIMMs inside the NVRAM module. To replace a failed NVRAM module, you must remove it from the chassis, remove the FlashCache module or modules from the NVRAM module, move the DIMMs to the replacement module, reinstall the FlashCache module or modules, and install the replacement NVRAM module into the chassis. Because the system ID is derived from the NVRAM module, if replacing the module, disks belonging to the system are reassigned to the new system ID.

Before you begin

- All disk shelves must be working properly.
- If your system is in an HA pair, the partner node must be able to take over the node associated with the NVRAM module that is being replaced.
- This procedure uses the following terminology:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy* node is the HA partner of the impaired node.
- This procedure includes steps for automatically or manually reassigning disks to the controller module associated with the new NVRAM module. You must reassign the disks when directed to in the procedure. Completing the disk reassignment before giveback can cause issues.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You cannot change any disks or disk shelves as part of this procedure.

Step 1: Shut down the impaired controller

```
Shut down or take over the impaired controller using one of the following
options.
```

Option 1: Most systems

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a Two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace the NVRAM module

To replace the NVRAM module, locate it in slot 6 in the chassis and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Move the FlashCache module from the old NVRAM module to the new NVRAM module:

1	Orange release button (gray on empty FlashCache modules)
2	FlashCache cam handle

a. Press the orange button on the front of the FlashCache module.

> The release button on empty FlashCache modules is gray.

b. Swing the cam handle out until the module begins to slide out of the old NVRAM module.

c. Grasp the module cam handle and slide it out of the NVRAM module and insert it into the front of the new NVRAM module.

d. Gently push the FlashCache module all the way into the NVRAM module, and then swing the cam handle closed until it locks the module in place.

3. Remove the target NVRAM module from the chassis:

a. Depress the lettered and numbered cam button.

The cam button moves away from the chassis.

b. Rotate the cam latch down until it is in a horizontal position.

The NVRAM module disengages from the chassis and moves out a few inches.

c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

1	Lettered and numbered I/O cam latch
2	I/O latch completely unlocked

4. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.

1	Cover locking button
2	DIMM and DIMM ejector tabs

5. Remove the DIMMs, one at a time, from the old NVRAM module and install them in the replacement NVRAM module.
6. Close the cover on the module.
7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

Step 3: Replace a NVRAM DIMM

To replace NVRAM DIMMs in the NVRAM module, you must remove the NVRAM module, open the module, and then replace the target DIMM.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The NVRAM module disengages from the chassis and moves out a few inches.

c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

1	Lettered and numbered I/O cam latch
2	I/O latch completely unlocked

3. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.

1	Cover locking button
2	DIMM and DIMM ejector tabs

4. Locate the DIMM to be replaced inside the NVRAM module, and then remove it by pressing down on the DIMM locking tabs and lifting the DIMM out of the socket.

   Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.
6. Close the cover on the module.
7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

Step 4: Reboot the controller after FRU replacement

After you replace the FRU, you must reboot the controller module.

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Reassign disks

Depending on whether you have an HA pair or two-node MetroCluster configuration, you must either verify the reassignment of disks to the new controller module or manually reassign the disks.

Select one of the following options for instructions on how to reassign disks to the new controller.

Option 1: Verify ID (HA pair)

Verify the system ID change on an HA system

You must confirm the system ID change when you boot the *replacement* node and then verify that the change was implemented.

This procedure applies only to systems running ONTAP in an HA pair.

Steps

1. If the replacement node is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the replacement node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.

   ```
   boot_ontap bye
   ```

   The node will reboot, if autoboot is set.

3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

   In the command output, you should see a message that the system ID has changed on the impaired node, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

   ```
   node1> `storage failover show`
                                        Takeover
   Node              Partner            Possible     State Description
   ------------      ------------       --------
   -------------------------------------
   node1             node2              false        System ID changed
   on partner (Old:
                                                     151759755, New:
   151759706), In takeover
   node2             node1              -            Waiting for
   giveback (HA mailboxes)
   ```

4. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore`command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command: `system`

```
node run -node local-node-name partner savecore -s
```

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

   a. From the healthy node, give back the replaced node's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* node takes back its storage and completes booting.

      If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.

      > If the giveback is vetoed, you can consider overriding the vetoes.

      Find the High-Availability Configuration Guide for your version of ONTAP 9

   b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

      The output from the `storage failover show` command should not include the `System ID changed on partner` message.

6. Verify that the disks were assigned correctly: `storage disk show -ownership`

   The disks belonging to the *replacement* node should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> `storage disk show -ownership`

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home
ID Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------
---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -
1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the node: `metrocluster node show`

   The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each node will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the node is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a node on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* node is the current owner of the disks on the disaster site.

     Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

9. If your system is in a MetroCluster configuration, verify that each node is configured: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

10. Verify that the expected volumes are present for each node: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Option 2: Reassign ID (MetroCluster config)

Reassign the system ID in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired* node is the node on which you are performing maintenance.
- The *replacement* node is the new node that replaced the impaired node as part of this procedure.
- The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering

`Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid,dr-partner-systemid`

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

```
dr-group-id cluster         node                 node-systemid dr-
partner-systemid
 ----------- --------------------- --------------------
------------- -------------------
 1           Cluster_A             Node_A_1             536872914
118073209
 1           Cluster_B             Node_B_1             118073209
536872914
 2 entries were displayed.
```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

   In this example, the new system ID is 118065481:

```
Local System ID: 118065481
    ...
    ...
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER                  POOL   SERIAL NUMBER  HOME
-------    -------------          -----  -------------  -------------
disk_name   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Verify that the coredumps are saved: `system node run -node` *`local-node-name`* `partner savecore`

      If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node` *`local-node-name`* `partner savecore -s command`.</info>.

   c. Return to the admin privilege level: `set -privilege admin`
7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

```
node1_siteA::> metrocluster node show -fields configuration-state

dr-group-id            cluster node           configuration-state
-----------            ---------------------- --------------
-------------------
1 node1_siteA          node1mcc-001           configured
1 node1_siteA          node1mcc-002           configured
1 node1_siteB          node1mcc-003           configured
1 node1_siteB          node1mcc-004           configured

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:
    a. Check for any health alerts on both clusters: `system health alert show`
    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`
    c. Perform a MetroCluster check: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
12. Simulate a switchover operation:
    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

       You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).
    b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`
    c. Return to the admin privilege level: `set -privilege admin`

Step 6: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use one of the following procedures, depending on whether you are using onboard or external key

management:

- Restore onboard key management encryption keys
- Restore external key management encryption keys

Step 7: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Swap out a power supply - AFF A700 and FAS9000

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

> Do not mix PSUs with different efficiency ratings. Always replace like for like.

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
   a. Turn off the power switch on the power supply.
   b. Open the power cable retainer, and then unplug the power cable from the power supply.
   c. Unplug the power cable from the power source.
4. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.

> When removing a power supply, always use two hands to support its weight.

1	Locking button

5. Make sure that the on/off switch of the new power supply is in the Off position.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

   The power supplies are keyed and can only be installed one way.

   > Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Reconnect the power supply cabling:

   a. Reconnect the power cable to the power supply and the power source.

   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.

8. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

   The green power LED lights when the PSU is fully inserted into the chassis and the amber attention LED flashes initially, but turns off after a few moments.

9. After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace the real-time clock battery

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization

continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

If you 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 Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 2: Controller is in a MetroCluster

> Do not use this procedure if your system is in a two-node MetroCluster configuration.

To shut down the impaired controller, you must determine the status of the controller and, if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Option 3: Controller is in a two-node MetroCluster

To shut down the impaired controller, you must determine the status of the controller and, if necessary, switch over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

1	Controller module cover locking button

Step 3: Replace the RTC battery

To replace the RTC battery, you must locate the failed battery in the controller module, remove it from the holder, and then install the replacement battery in the holder.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.

1	RTC battery
2	RTC battery housing

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

> Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
8. Reinstall the controller module cover.

Step 4: Reinstall the controller module and set time/date

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

Steps

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the system, as needed.

   If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

      Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
   e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy node with the `show date` command.
   b. At the LOADER prompt on the target node, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target node.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the node reboot.
8. Return the node to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

X91148A module

Overview of adding an X91148A module - AFF A9000

You can add an I/O module to your system by either replacing a NIC or storage adapter with a new one in a fully-populated system, or by adding a new NIC or storage adapter into an empty chassis slot in your system.

Before you begin

- Check the NetApp Hardware Universe to make sure that the new I/O module is compatible with your system and version of ONTAP you're running.
- If multiple slots are available, check the slot priorities in NetApp Hardware Universe and use the best one available for your I/O module.
- To non-disruptively add an I/O module, you must takeover the target controller, remove the slot blanking cover in the target slot or remove an existing I/O module, add the new or replacement I/O module, and then giveback the target controller.
- Make sure that all other components are functioning properly.

Add an X91148A module in an AFF A700 with open slots - AFF A700 and FAS9000

You can add an X91148A module into an empty module slot in your system as either a 100GbE NIC or a storage module for the NS224 storage shelves.

- Your system must be running ONTAP 9.8 and later.
- To non-disruptively add the X91148A module, you must takeover the target controller, remove the slot blanking cover in the target slot, add the module, and then giveback the target controller.
- There must be one or more open slots available on your system.
- If multiple slots are available, install the module according to the slot priority matrix for the X91148A module in the Hardware Universe.

  NetApp Hardware Universe

- If you are adding the X91148A module as a storage module, you must install the module slots 3 and/or 7.
- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` command. See the Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

- All other components in the system must be functioning properly; if not, you must contact technical support.

Option 1: Add an X91148A module as a NIC module in a system with open slots

To add an X91148A module as a NIC module in a system with open slots, you must follow the specific sequence of steps.

Steps

1. Shutdown controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode` *`target_node_name`*

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.
2. If you are not already grounded, properly ground yourself.
3. Remove the target slot blanking cover:
   a. Depress the lettered and numbered cam button.
   b. Rotate the cam latch down until it is in a horizontal position.
   c. Remove the blanking cover.
4. Install the X91148A module:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
5. Cable the module to the data switches.
6. Reboot controller A: `boot_ontap`
7. Giveback the node from the partner node: `storage failover giveback -ofnode` *`target_node_name`*
8. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
9. Repeat these steps for controller B.

Option 2: Add an X91148A module as a storage module in a system with open slots

To add an X91148A module as a storage module in a system with open slots, you must follow the specific sequence of steps.

- This procedure presumes slots 3 and/or 7 are open.

Steps

1. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

2. If you are not already grounded, properly ground yourself.
3. Remove the target slot blanking cover:
   a. Depress the lettered and numbered cam button.
   b. Rotate the cam latch down until it is in a horizontal position.
   c. Remove the blanking cover.
4. Install the X91148A module into slot 3:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
   d. If you are installing a second X91148A module for storage, repeat this step for the module in slot 7.
5. Reboot controller A: `boot_ontap`
6. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`
7. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
8. Repeat these steps for controller B.
9. Install and cable your NS224 shelves, as described in Hot-add - NS224 shelves.

Add an X91148A storage module in a system with no open slots - AFF A700 and FAS9000

You must remove one more or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- Your system must be running ONTAP 9.8 and later.
- To non-disruptively add the X91148A module, you must takeover the target controller, add the module, and then giveback the target controller.
- If you are adding the X91148A module as a storage adapter, you must install the module in slots 3 and/or 7.
- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` command for each port. See the Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

- All other components in the system must be functioning properly; if not, you must contact technical support.

Option 1: Add an X91148A module as a NIC module in a system with no open slots

You must remove one or more existing NIC or storage modules in your system in order to

install one or more X91148A NIC modules into your fully-populated system.

Steps

1. If you are adding an X91148A module into a slot that contains a NIC module with the same number of ports as the X91148A module, the LIFs will automatically migrate when its controller module is shut down. If the NIC module being replaced has more ports than the X91148A module, you must permanently reassign the affected LIFs to a different home port. See Migrating a LIF for information about using System Manager to permanently move the LIFs
2. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode` *`target_node_name`*

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.
3. If you are not already grounded, properly ground yourself.
4. Unplug any cabling on the target I/O module.
5. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.
   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

6. Install the X91148A module into the target slot:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
7. Repeat the remove and install steps to replace additional modules for controller A.
8. Cable the module or modules to the data switches.
9. Reboot controller A: `boot_ontap`
10. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`
11. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
12. If you added the X91148A module as a NIC module in slots 3 or 7, for networking, use the `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` command for each port.
13. Repeat these steps for controller B.

Option 2: Adding an X91148A module as a storage module in a system with no open slots

You must remove one or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- This procedure presumes you re installing the X91148A module into slots 3 and/or 7.

Steps

1. If you are adding an X91148A module as a storage module in slots 3 and/or 7 into a slot that has an existing NIC module in it, use System Manager to permanently migrate the LIFs to different home ports, as described in Migrating a LIF.
2. Shut down controller A:
   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.
3. If you are not already grounded, properly ground yourself.
4. Unplug any cabling on the target I/O module.
5. Remove the target I/O module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.
   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

6. Install the X91148A module into slot 3:
   a. Align the X91148A module with the edges of the slot.
   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
   c. Push the I/O cam latch all the way up to lock the module in place.
   d. If you are installing a second X91148A module for storage, repeat the remove and install steps for the module in slot 7.
7. Reboot controller A: `boot_ontap`
8. Giveback the node from the partner node: `storage failover giveback -ofnode` *`target_node_name`*
9. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
10. Repeat these steps for controller B.
11. Install and cable your NS224 shelves, as described in Hot-adding an NS224 drive shelf.

All SAN Array systems

You can use the AFF documentation with your ASA system. The information for AFF models applies to the corresponding ASA system. For example, all cabling and other information for the AFF A400 system also applies to the ASA AFF A400 system.

All SAN Array Software Configuration

Upgrade procedures

For most AFF and FAS systems, follow the upgrade procedures found on the Upgrade AFF and FAS Systems Doc site.

For systems in a MetroCluster configuration, follow the the upgrade procedures found on the ONTAP MetroCluster Doc site.

System-level diagnostics

Introduction to system-level diagnostics

System-level diagnostics provides a command-line interface for tests that search for and determine hardware problems on supported storage systems. You use system-level diagnostics to confirm that a specific component is operating properly or to help identify faulty components.

System-level diagnostics is available for supported storage systems only. Entering system-level diagnostics at the command-line interface of unsupported storage systems generates an error message.

You run system-level diagnostics after one of the following common troubleshooting situations:

- Initial system installation
- Addition or replacement of hardware components
- System panic caused by an unidentified hardware failure
- Access to a specific device becomes intermittent or the device becomes unavailable
- System response time becomes sluggish

To run system-level diagnostics, you must already be running Data ONTAP because you need to reach the **Maintenance mode boot** option in Data ONTAP. There are several approaches to get to this option, but this is the recommended approach taken in the procedures documented in this guide. Some hardware components in your system may require a specific approach, and this would be documented in the applicable field replaceable unit (FRU) flyer. This guide does not provide detailed definitions of specific commands, subcommands, tests, or conditions.

Once the command is entered, the tests run in the background and the passed or failed outcome of the tests is logged in the internal memory-based log, which has a fixed size. Some tests are utilities and will simply state completed rather than passed or failed. After you run the appropriate tests, the procedures documented in this guide help you generate status report. Once the test results show a successful completion of system-level diagnostics, it is a recommended best practice to clear the log.

In the event of test failures, the status reports will help technical support make appropriate recommendations. The failure could be resolved by reinstalling the FRU, by ensuring cables are connected, or by enabling specific tests recommended by technical support and then re-running those tests. If the failure cannot be resolved, then there is a hardware failure and the affected hardware must be replaced.

There are no error messages that require further definitions or explanations.

Requirements for running system-level diagnostics

Depending on the system-level diagnostic tests you are running, you need to be aware of time and system hardware requirements.

Each documented task has slight differences; use the recommended procedure for the task.

The following requirements must be met when running system-level diagnostics; otherwise, parts of the tests fail and error messages appear in the status report:

General requirements

- Each system being tested must be on a separate network.

  The network interface test assigns unique static IP addresses, beginning with 172.25.150.23, to all available network interfaces on a storage system. This results in network interface ports on different storage controllers being assigned the same IP address. If all the systems being tested are on the same network, then duplicate ip address warning messages appear on the connected consoles. These warning messages do not affect the test results.

System memory requirements

- You need to set aside time when running memory tests; the larger the memory capacity of your storage system, the longer it takes.

NIC requirements

- All adjacent network interface ports on the system must be connected for best performance using a standard Ethernet cable.

  Examples of adjacent ports are e0a and e0b or e2c and e2d.

  > e0M and e0P ports cannot be connected together due to an internal switch connection. In systems with e0M and e0P ports, the most efficient pairings are e0M with e0a and e0P with e0b.

- If there are a number of network interface ports on the system, you may need to run the NIC system-level diagnostic test several times, limiting each run to no more than two pairs each time.

SAS requirements

- When running the SAS system-level diagnostic tests, adjacent SAS ports must be connected for best performance; storage shelves must be disconnected from the ports.

  > Connections between adjacent SAS ports is no longer a requirement for systems running Data ONTAP 8.2; however, only the internal loopback test will be run for systems with unconnected SAS ports.

FC-AL requirements

- When running the FC-AL system-level diagnostic tests, you must have loopback hoods on FC-AL interfaces on the motherboard or expansion adapters for best performance; all other cables for storage or Fibre Channel networks must be disconnected from the ports.

  > While the use of loopback hoods on FC-AL interfaces are no longer requirements for systems running Data ONTAP 8.2, the scope of the test coverage on the interface is also reduced.

CNA requirements

- The use of loopback hoods is not a requirement for running CNA system-level diagnostics tests.

Interconnect requirements

- Both platform controller modules in a dual controller system must be in Maintenance mode for the interconnect system-level diagnostic test to run.

> You will receive a warning message if you attempt to run the interconnect system-level diagnostic test with other system-level diagnostic tests.

How to use online command-line help

You can get command-line syntax help from the command line by entering the name of the command followed by help or the question mark (?).

The fonts or symbols used in syntax help are as follows:

- **keyword**

  Specifies the name of a command or an option that must be entered as shown.

- **< > (less than, greater than symbols)**

  Specify that you must replace the variable identified inside the symbols with a value.

- **| (pipe)**

  Indicates that you must choose one of the elements on either side of the pipe.

- **[ ] (brackets)**

  Indicate that the element inside the brackets is optional.

- **{ } (braces)**

  Indicate that the element inside the braces is required.

You can also type the question mark at the command line for a list of all the commands that are available at the current level of administration (administrative or advanced).

The following example shows the result of entering the environment help command at the storage system command line. The command output displays the syntax help for the environment commands.

```
toaster> environment help
Usage: environment status |
[status] [shelf [<adapter>]] |
[status] [shelf_log] |
[status] [shelf_stats] |
[status] [shelf_power_status] |
[status] [chassis [all | list-sensors | Fan | Power | Temp | Power Supply
| RTC Battery | NVRAM4-temperature-7 | NVRAM4-battery-7]]
```

Run system installation diagnostics

You run diagnostics after an initial system installation to identify the version of system-level diagnostics and the supported devices on your storage system, and to verify that the installation is successful and that all hardware is functioning properly.

Your storage system must already be running Data ONTAP.

1. At the storage system prompt, switch to the LOADER prompt: `halt`
2. Enter the following command at the LOADER prompt: `boot_diags`

   > You must run this command from the LOADER prompt for system-level diagnostics to function properly. The boot_diags command starts special drivers designed specifically for system-level diagnostics.

3. View the version of system-level diagnostics present on your storage system by entering the following command: `sldiag version show`

   The version is displayed in the format System Level DiagnosticsX.nn.nn. The X is an alpha reference and nn.nn are major and minor numeric references, respectively.

4. Identify the device types in your new system installation so that you know which components to verify by entering the following command: `sldiag device types`

   Your storage system displays some or all of the following devices:

   - `ata` is an Advanced Technology Attachment device.
   - `bootmedia` is the system booting device.
   - `cna` is a Converged Network Adapter not connected to a network or storage device.
   - `env` is motherboard environmentals.
   - `fcache` is the Flash Cache adapter, also known as the Performance Acceleration Module 2.
   - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a storage device or Fibre Channel network.
   - `fcvi` is the Fiber Channel Virtual Interface not connected to a Fibre Channel network.
   - `interconnect` or `nvram-ib` is the high-availability interface.

- mem is system memory.
- `nic` is a Network Interface Card not connected to a network.
- `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.
- `serviceproc` is the Service Processor.
- `storage` is an ATA, FC-AL, or SAS interface that has an attached disk shelf.
- `toe` is a TCP Offload Engine, a type of NIC.

5. Run all the default selected diagnostic tests on your storage system by entering the following command: `sldiag device run`
6. View the status of the test by entering the following command: `sldiag device status`

   Your storage system provides the following output while the tests are still running:

   ```
   There are still test(s) being processed.
   ```

   After all the tests are complete, the following response appears by default:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

7. Verify that there are no hardware problems on your new storage system by entering the following command: `sldiag device status -long -state failed`

   The following example shows how the full status of the failures is displayed in a test run without the appropriate hardware:

   ```
   *> **sldiag device status -long -state failed**

   TEST START -------------------------------------------
   DEVTYPE: nvram_ib
   NAME: external  loopback test
   START DATE: Sat Jan  3 23:10:55 GMT 2009

   STATUS: Completed
   ib3a: could not set loopback mode, test failed
   END DATE: Sat Jan  3 23:11:04 GMT 2009

   LOOP: 1/1
   TEST END ---------------------------------------------

   TEST START -------------------------------------------
   DEVTYPE: fcal
   ```

```
NAME: Fcal Loopback Test
START DATE: Sat Jan  3 23:10:56 GMT 2009

STATUS: Completed
Starting test on Fcal Adapter: 0b
Started gathering adapter info.
Adapter get adapter info OK
Adapter fc_data_link_rate: 1Gib
Adapter name: QLogic 2532
Adapter firmware rev: 4.5.2
Adapter hardware rev: 2

Started adapter get WWN string test.
Adapter get WWN string OK wwn_str: 5:00a:098300:035309

Started adapter interrupt test
Adapter interrupt test OK

Started adapter reset test.
Adapter reset OK

Started Adapter Get Connection State Test.
Connection State: 5
Loop on FC Adapter 0b is OPEN

Started adapter Retry LIP test
Adapter Retry LIP OK

ERROR: failed to init adaptor port for IOCTL call

ioctl_status.class_type = 0x1

ioctl_status.subclass = 0x3

ioctl_status.info = 0x0
 Started INTERNAL LOOPBACK:
INTERNAL LOOPBACK   OK
Error Count: 2  Run Time: 70 secs
>>>>> ERROR, please ensure the port has a shelf or plug.
END DATE: Sat Jan  3 23:12:07 GMT 2009

LOOP: 1/1
TEST END ---------------------------------------------
```

If the system-level diagnostics tests…	Then…
Were completed without any failures	There are no hardware problems and your storage system returns to the prompt. a. Clear the status logs by entering the following command: `sldiag device clearstatus` b. Verify that the log is cleared by entering the following command: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode by entering the following command: `halt` d. Enter the following command at the Loader prompt to boot the storage system: `boot_ontap` You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode by entering the following command: `halt` b. Perform a clean shutdown and disconnect the power supplies. 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. d. Reconnect the power supplies and power on the storage system. e. Repeat Steps 1 through 7 of *Running system installation diagnostics*.

Run system panic diagnostics

Running diagnostics after your storage system suffers a system panic can help you to identify the possible cause of the panic.

1. At the storage system prompt, switch to the LOADER prompt: `halt`
2. Enter the following command at the LOADER prompt: `boot_diags`

   You must run this command from the LOADER prompt for system-level diagnostics to function properly. The boot_diags command starts special drivers designed specifically for system-level diagnostics.

3. Run diagnostics on all the devices by entering the following command: `sldiag device run`

4. View the status of the test by entering the following command: `sldiag device status`

   Your storage system provides the following output while the tests are still running:

   ```
   There are still test(s) being processed.
   ```

   After all the tests are complete, you receive the following default response:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

5. Identify the cause of the system panic by entering the following command: `sldiag device status -long -state failed`

   The following example shows how the full status of the failures is displayed in a test run without the appropriate hardware:

   ```
   *> **sldiag device status -long -state failed**

   TEST START -------------------------------------------
   DEVTYPE: nvram_ib
   NAME: external  loopback test
   START DATE: Sat Jan  3 23:10:55 GMT 2009

   STATUS: Completed
   ib3a: could not set loopback mode, test failed
   END DATE: Sat Jan  3 23:11:04 GMT 2009

   LOOP: 1/1
   TEST END ---------------------------------------------

   TEST START -------------------------------------------
   DEVTYPE: fcal
   NAME: Fcal Loopback Test
   START DATE: Sat Jan  3 23:10:56 GMT 2009

   STATUS: Completed
   Starting test on Fcal Adapter: 0b
   Started gathering adapter info.
   Adapter get adapter info OK
   Adapter fc_data_link_rate: 1Gib
   Adapter name: QLogic 2532
   Adapter firmware rev: 4.5.2
   Adapter hardware rev: 2

   Started adapter get WWN string test.
   ```

```
Adapter get WWN string OK wwn_str: 5:00a:098300:035309

Started adapter interrupt test
Adapter interrupt test OK

Started adapter reset test.
Adapter reset OK

Started Adapter Get Connection State Test.
Connection State: 5
Loop on FC Adapter 0b is OPEN

Started adapter Retry LIP test
Adapter Retry LIP OK

ERROR: failed to init adaptor port for IOCTL call

ioctl_status.class_type = 0x1

ioctl_status.subclass = 0x3

ioctl_status.info = 0x0
 Started INTERNAL LOOPBACK:
INTERNAL LOOPBACK   OK
Error Count: 2  Run Time: 70 secs
>>>>> ERROR, please ensure the port has a shelf or plug.
END DATE: Sat Jan  3 23:12:07 GMT 2009

LOOP: 1/1
TEST END ---------------------------------------------
```

If the system-level diagnostics tests…	Then…
Were completed without any failures	There are no hardware problems and your storage system returns to the prompt. a. Clear the status logs by entering the following command: `sldiag device clearstatus` b. Verify that the log is cleared by entering the following command: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode by entering the following command: `halt` d. Enter the following command at the Loader prompt to boot the storage system: `boot_ontap` You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode by entering the following command: `halt` b. Perform a clean shutdown and disconnect the power supplies. 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. d. Reconnect the power supplies and power on the storage system. e. Repeat Steps 1 through 5 of *Running system panic diagnostics*.

If the failures persist after repeating the steps, you need to replace the hardware.

Run slow system response diagnostics

Running diagnostics can help you identify the causes of slow system response times.

1. At the storage system prompt, switch to the LOADER prompt: `halt`
2. Enter the following command at the LOADER prompt: `boot_diags`

> You must run this command from the LOADER prompt for system-level diagnostics to function properly. The boot_diags command starts special drivers designed specifically for system-level diagnostics.

3. Run diagnostics on all the devices by entering the following command: `sldiag device run`

4. View the status of the test by entering the following command: `sldiag device status`

   Your storage system provides the following output while the tests are still running:

   ```
   There are still test(s) being processed.
   ```

   After all the tests are complete, the following response appears by default:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

5. Identify the cause of the system sluggishness by entering the following command: `sldiag device status -long -state failed`

   The following example shows how the full status of the failures is displayed in a test run without the appropriate hardware:

   ```
   *> **sldiag device status -long -state failed**

   TEST START -------------------------------------------
   DEVTYPE: nvram_ib
   NAME: external  loopback test
   START DATE: Sat Jan  3 23:10:55 GMT 2009

   STATUS: Completed
   ib3a: could not set loopback mode, test failed
   END DATE: Sat Jan  3 23:11:04 GMT 2009

   LOOP: 1/1
   TEST END ---------------------------------------------

   TEST START -------------------------------------------
   DEVTYPE: fcal
   NAME: Fcal Loopback Test
   START DATE: Sat Jan  3 23:10:56 GMT 2009

   STATUS: Completed
   Starting test on Fcal Adapter: 0b
   Started gathering adapter info.
   Adapter get adapter info OK
   Adapter fc_data_link_rate: 1Gib
   Adapter name: QLogic 2532
   Adapter firmware rev: 4.5.2
   Adapter hardware rev: 2

   Started adapter get WWN string test.
   ```

```
Adapter get WWN string OK wwn_str: 5:00a:098300:035309

Started adapter interrupt test
Adapter interrupt test OK

Started adapter reset test.
Adapter reset OK

Started Adapter Get Connection State Test.
Connection State: 5
Loop on FC Adapter 0b is OPEN

Started adapter Retry LIP test
Adapter Retry LIP OK

ERROR: failed to init adaptor port for IOCTL call

ioctl_status.class_type = 0x1

ioctl_status.subclass = 0x3

ioctl_status.info = 0x0
 Started INTERNAL LOOPBACK:
INTERNAL LOOPBACK   OK
Error Count: 2  Run Time: 70 secs
>>>>> ERROR, please ensure the port has a shelf or plug.
END DATE: Sat Jan  3 23:12:07 GMT 2009

LOOP: 1/1
TEST END ---------------------------------------------
```

If the system-level diagnostics tests…	Then…
Were completed without any failures	There are no hardware problems and your storage system returns to the prompt. a. Clear the status logs by entering the following command: `sldiag device clearstatus` b. Verify that the log is cleared by entering the following command: `sldiag device status` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode by entering the following command: `halt` d. Enter the following command at the Loader prompt to boot the storage system: `boot_ontap` You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode by entering the following command: `halt` b. Perform a clean shutdown and disconnect the power supplies. c. Verify that you observed all the requirements for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies and power on the storage system. e. Repeat Steps 1 through 5 of *Running slow system response diagnostics*.

If the system-level diagnostics tests…	Then…
Resulted in the same test failures	Technical support might recommend modifying the default settings on some of the tests to help identify the problem. a. Modify the selection state of a specific device or type of device on your storage system by entering the following command: `sldiag device modify [-dev devtype|mb|slot_slotnum_] [-name device] [-selection enable|disable|default|only]` `-selection enable|disable|default|only` allows you to enable, disable, accept the default selection of a specified device type or named device, or only enable the specified device or named device by disabling all others first. b. Verify that the tests were modified by entering the following command: `sldiag option show` c. Repeat Steps 3 through 5 of *Running slow system response diagnostics*. d. After you identify and resolve the problem, reset the tests to their default states by repeating substeps 1 and 2. e. Repeat Steps 1 through 5 of *Running slow system response diagnostics*.

If the failures persist after repeating the steps, you need to replace the hardware.

Run hardware installation diagnostics

You run diagnostics after adding or replacing hardware components in your storage system to verify that the component has no problems and that the installation is successful.

1. At the storage system prompt, switch to the LOADER prompt: `halt`
2. Enter the following command at the LOADER prompt: `boot_diags`

> You must run this command from the LOADER prompt for system-level diagnostics to function properly. The boot_diags command starts special drivers designed specifically for system-level diagnostics.

3. Run the default tests on the particular device you added or replaced by entering the following command: `sldiag device run [-dev devtype|mb|slotslotnum] [-name device]`
   - -dev devtype specifies the type of device to be tested.
     - `ata` is an Advanced Technology Attachment device.
     - `bootmedia` is the system booting device..

        - `cna` is a Converged Network Adapter not connected to a network or storage device.
        - `env` is motherboard environmentals.
        - `fcache` is the Flash Cache adapter, also known as the Performance Acceleration Module 2.
        - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a storage device or Fibre Channel network.
        - `fcvi` is the Fiber Channel Virtual Interface not connected to a Fibre Channel network.
        - `interconnect` or `nvram-ib` is the high-availability interface.
        - `mem` is system memory.
        - `nic` is a Network Interface Card not connected to a network.
        - `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.
        - `serviceproc` is the Service Processor.
        - `storage` is an ATA, FC-AL, or SAS interface that has an attached disk shelf.
        - `toe` is a TCP Offload Engine, a type of NIC.
    - `mb` specifies that all the motherboard devices are to be tested.
    - `slot` *`slotnum`* specifies that a device in a specific slot number is to be tested.
    - `-name` *`device`* specifies a given device class and type.
4. View the status of the test by entering the following command: `sldiag device status`

   Your storage system provides the following output while the tests are still running:

   ```
   There are still test(s) being processed.
   ```

   After all the tests are complete, the following response appears by default:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

5. Verify that no hardware problems resulted from the addition or replacement of hardware components on your storage system by entering the following command: `sldiag device status [-dev devtype|mb|slotslotnum] [-name device] -long -state failed`

   The following example pulls up the full status of failures resulting from testing a newly installed FC-AL adapter:

   ```
   *> **sldiag device status -dev fcal -long -state failed**

   TEST START ------------------------------------------
   DEVTYPE: fcal
   ```

```
NAME: Fcal Loopback Test
START DATE: Sat Jan  3 23:10:56 GMT 2009

STATUS: Completed
Starting test on Fcal Adapter: 0b
Started gathering adapter info.
Adapter get adapter info OK
Adapter fc_data_link_rate: 1Gib
Adapter name: QLogic 2532
Adapter firmware rev: 4.5.2
Adapter hardware rev: 2

Started adapter get WWN string test.
Adapter get WWN string OK wwn_str: 5:00a:098300:035309

Started adapter interrupt test
Adapter interrupt test OK

Started adapter reset test.
Adapter reset OK

Started Adapter Get Connection State Test.
Connection State: 5
Loop on FC Adapter 0b is OPEN

Started adapter Retry LIP test
Adapter Retry LIP OK

ERROR: failed to init adaptor port for IOCTL call

ioctl_status.class_type = 0x1

ioctl_status.subclass = 0x3

ioctl_status.info = 0x0
 Started INTERNAL LOOPBACK:
INTERNAL LOOPBACK   OK
Error Count: 2  Run Time: 70 secs
>>>>> ERROR, please ensure the port has a shelf or plug.
END DATE: Sat Jan  3 23:12:07 GMT 2009

LOOP: 1/1
TEST END ---------------------------------------------
```

If the system-level diagnostics tests…	Then…
Were completed without any failures	There are no hardware problems and your storage system returns to the prompt. a. Clear the status logs by entering the following command: `sldiag device clearstatus [-dev devtype
mb	slotslotnum]` .. Verify that the log is cleared by entering the following command: `sldiag device status [-dev devtype
mb	slotslotnum]` + The following default response is displayed: + ---- SLDIAG: No log messages are present. ----  .. Exit Maintenance mode by entering the following command: `halt` .. Enter the following command at the Loader prompt to boot the storage system: `boot_ontap` You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode by entering the following command: `halt` b. Perform a clean shutdown and disconnect the power supplies. 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. d. Reconnect the power supplies and power on the storage system. e. Repeat Steps 1 through 6 of *Running hardware installation diagnostics*.

If the failures persist after repeating the steps, you need to replace the hardware.

Run device failure diagnostics

Running diagnostics can help you determine why access to a specific device becomes intermittent or why the device becomes unavailable in your storage system.

1. At the storage system prompt, switch to the LOADER prompt: `halt`
2. Enter the following command at the LOADER prompt: `boot_diags`

> You must run this command from the LOADER prompt for system-level diagnostics to function properly. The boot_diags command starts special drivers designed specifically for system-level diagnostics.

3. Run diagnostics on the device causing problems by entering the following command: `sldiag device run [-dev devtype|mb|slotslotnum] [-name device]`
   - -dev *devtype* specifies the type of device to be tested.
     - `ata` is an Advanced Technology Attachment device.
     - `bootmedia` is the system booting device..
     - `cna` is a Converged Network Adapter not connected to a network or storage device.
     - `env` is motherboard environmentals.
     - `fcache` is the Flash Cache adapter, also known as the Performance Acceleration Module 2.
     - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a storage device or Fibre Channel network.
     - `fcvi` is the Fiber Channel Virtual Interface not connected to a Fibre Channel network.
     - `interconnect` or `nvram-ib` is the high-availability interface.
     - `mem` is system memory.
     - `nic` is a Network Interface Card not connected to a network.
     - `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.
     - `serviceproc` is the Service Processor.
     - `storage` is an ATA, FC-AL, or SAS interface that has an attached disk shelf.
     - `toe` is a TCP Offload Engine, a type of NIC.
   - `mb` specifies that all the motherboard devices are to be tested.
   - `slot`*slotnum* specifies that a device in a specific slot number is to be tested.
   - `-name` *`device`* specifies a given device class and type.
4. View the status of the test by entering the following command: `sldiag device status`

   Your storage system provides the following output while the tests are still running:

   ```
   There are still test(s) being processed.
   ```

   After all the tests are complete, the following response appears by default:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

5. Identify any hardware problems by entering the following command: `sldiag device status [-dev devtype|mb|slotslotnum] [-name device] -long -state failed`

   The following example shows how the full status of failures resulting from testing the FC-AL adapter are displayed:

```
*> **sldiag device status fcal -long -state failed**

TEST START ------------------------------------------
DEVTYPE: fcal
NAME: Fcal Loopback Test
START DATE: Sat Jan  3 23:10:56 GMT 2009

STATUS: Completed
Starting test on Fcal Adapter: 0b
Started gathering adapter info.
Adapter get adapter info OK
Adapter fc_data_link_rate: 1Gib
Adapter name: QLogic 2532
Adapter firmware rev: 4.5.2
Adapter hardware rev: 2

Started adapter get WWN string test.
Adapter get WWN string OK wwn_str: 5:00a:098300:035309

Started adapter interrupt test
Adapter interrupt test OK

Started adapter reset test.
Adapter reset OK

Started Adapter Get Connection State Test.
Connection State: 5
Loop on FC Adapter 0b is OPEN

Started adapter Retry LIP test
Adapter Retry LIP OK

ERROR: failed to init adaptor port for IOCTL call

ioctl_status.class_type = 0x1

ioctl_status.subclass = 0x3

ioctl_status.info = 0x0
 Started INTERNAL LOOPBACK:
INTERNAL LOOPBACK   OK
```

```
Error Count: 2  Run Time: 70 secs
>>>>> ERROR, please ensure the port has a shelf or plug.
END DATE: Sat Jan  3 23:12:07 GMT 2009

LOOP: 1/1
TEST END ---------------------------------------------
```

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode by entering the following command: `halt` b. Perform a clean shutdown and disconnect the power supplies. 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. d. Reconnect the power supplies and power on the storage system. e. Repeat Steps 1 through 5 of *Running device failure diagnostics*.
Resulted in the same test failures	Technical support might recommend modifying the default settings on some of the tests to help identify the problem. a. Modify the selection state of a specific device or type of device on your storage system by entering the following command: `sldiag device modify [-dev devtype|mb|slot_slotnum_] [-name device] [-selection enable|disable|default|only]` `-selection enable|disable|default|only` allows you to enable, disable, accept the default selection of a specified device type or named device, or only enable the specified device or named device by disabling all others first. b. Verify that the tests were modified by entering the following command: `sldiag option show` c. Repeat Steps 3 through 5 of *Running device failure diagnostics*. d. After you identify and resolve the problem, reset the tests to their `default` states by repeating substeps 1 and 2. e. Repeat Steps 1 through 5 of *Running device failure diagnostics*.

If the system-level diagnostics tests…	Then…
Were completed without any failures	There are no hardware problems and your storage system returns to the prompt. a. Clear the status logs by entering the following command: `sldiag device clearstatus [-dev devtype|mb|slot_slotnum_]` b. Verify that the log is cleared by entering the following command: `sldiag device status [-dev devtype|mb|slot_slotnum_]` The following default response is displayed: `SLDIAG: No log messages are present.` c. Exit Maintenance mode by entering the following command: `halt` d. Enter the following command at the Loader prompt to boot the storage system: `boot_ontap` You have completed system-level diagnostics.

If the failures persist after repeating the steps, you need to replace the hardware.

Drive shelves

NS224 shelves

Install and cable

Hot-add NS224 shelves

You can hot-add an NS224 drive shelf after your HA pair meets certain requirements, and after the preparation tasks applicable to your HA pair are completed.

Requirements for a hot-add

Your HA pair must meet certain requirements before hot-adding an NS224 drive shelf.

- Your platform model and version of ONTAP must support the NS224 shelf and drives you are hot-adding.

  NetApp Hardware Universe

- You must have the correct number and type of cables to connect the shelf.

  NetApp Hardware Universe

- Your HA pair must have enough available RoCE-capable ports to support the number of shelves you are hot-adding.

  For each shelf you are hot-adding, you need a minimum of two RoCE capable ports on each controller. These ports can be on board the controllers, on RoCE-capable PCIe cards, a combination of both, or on RoCE-capable I/O modules, as supported by your platform model.

  If your HA pair does not have enough available RoCE-capable ports, and your platform model supports the use of RoCE-capable PCIe cards or I/O modules, you must have installed the additional cards or I/O modules into the correct controller slots, as supported by your platform model.

  NetApp Hardware Universe

  > Non-dedicated RoCE-capable ports must be configured for storage use (not networking use).
  >
  > Prepare non-dedicated RoCE-capable ports for a hot-add

- If you have an AFF A700 HA pair and you are hot-adding the initial NS224 drive shelf (no NS224 drive shelf exists in your HA pair), you must have installed a core dump module (X9170A, NVMe 1TB SSD) in each controller to support core dumps (store core files).

  Replace the caching module or add/replace a core dump module — AFF A700 and FAS9000

- Your HA pair must have less than the maximum number of shelves supported, by at least the number of shelves you plan to hot-add.

  You cannot have exceeded the maximum number of shelves supported by your HA pair after hot-adding shelves.

NetApp Hardware Universe

- If you are hot-adding a shelf to an HA pair that already has an NS224 shelf, your HA pair cannot have any storage cabling error messages, and it must be cabled as multipath HA.

  You can run Active IQ Config Advisor to view any storage cabling error messages and the corrective actions you should take.

  NetApp Downloads: Config Advisor

- You need a paper clip with one side straightened or a narrow-tipped ballpoint pen.

  To change the shelf ID, you use the paper clip or ballpoint pen to access the shelf ID button behind the Operator Display Panel (ODP).

Considerations for a hot-add

You should familiarize yourself with best practices and aspects about this procedure before hot-adding an NS224 drive shelf.

- If you have an ASA HA pair supporting NS224 shelves, you can use this procedure.
- **Best practice:** The best practice is to have the current version of the Disk Qualification Package (DQP) installed before hot-adding a shelf.

  Having the current version of the DQP installed allows your system to recognize and use newly qualified drives. This avoids system event messages about having noncurrent drive information and prevention of drive partitioning because drives are not recognized. The DQP also notifies you of noncurrent drive firmware.

  NetApp Downloads: Disk Qualification Package

- **Best practice:** The best practice is to run Active IQ Config Advisor before and after hot-adding a shelf.

  Running Active IQ Config Advisor before hot-adding a shelf provides a snap shot of the existing shelf Ethernet (ENET) connectivity, verifies NVMe shelf module (NSM) firmware versions, and allows you to verify a shelf ID already in use in the HA pair. Running Active IQ Config Advisor after hot-adding a shelf allows you to verify shelves are cabled correctly and that shelf IDs are unique within the HA pair.

  NetApp Downloads: Config Advisor

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before adding a new shelf.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

  > Do not revert firmware to a version that does not support your shelf and its components.

- After you have cabled a hot-added shelf, ONTAP recognizes the shelf:
  - Drive ownership is assigned if automatic drive assignment is enabled.
  - NSM shelf firmware and drive firmware should be updated automatically, if needed.

Firmware updates can take up to 30 minutes.

Prepare for a hot-add

You must complete the preparation tasks applicable to your HA pair before hot-adding an NS224 drive shelf.

Prepare non-dedicated RoCE-capable ports for a hot-add

If your HA pair has non-dedicated RoCE-capable ports that you are using to hot-add an NS224 drive shelf, you must make sure the ports are configured for storage use (not networking use). Depending on your platform model, the RoCE-capable ports are on board the controllers, on RoCE-capable PCIe cards, a combination of both, or on RoCE-capable I/O modules.

Before you begin

You must have met the system requirements.

Requirements for a hot-add

About this task

- For some platform models, when a RoCE-capable PCIe card or I/O module is installed in a supported slot on a controller, the ports automatically default to storage use (instead of networking); however, it is recommended that you complete this procedure to verify the RoCE-capable ports are configured for storage use.
- If you determine that the non-dedicated RoCE-capable ports in your HA pair are not configured for storage use, it is a nondisruptive procedure to configure them.

If your HA pair is running a version of ONTAP 9.6, you need to reboot the controllers, one at a time.

If your HA pair is running ONTAP 9.7 or later, you do not need to reboot the controllers, unless one or both controllers are in maintenance mode. This procedure assumes that neither controller is in maintenance mode.

Steps

1. Verify if the non-dedicated ports in the HA pair are configured for storage use: `storage port show`

   You can enter the command on either controller module.

   If your HA pair is running ONTAP 9.8 or later, the non-dedicated ports display `storage` in the `Mode` column.

   If your HA pair is running ONTAP 9.7 or 9.6, the non-dedicated ports, which display `false` in the `Is Dedicated?` column, also display `enabled` in the `State` column.

2. If the non-dedicated ports are configured for storage use, you are done with this procedure.

   Otherwise, you need to configure the ports by completing steps 3 through 6.

When non-dedicated ports are not configured for storage use, the command output displays the following:

If your HA pair is running ONTAP 9.8 or later, the non-dedicated ports display `network` in the `Mode` column.

If your HA pair is running ONTAP 9.7 or 9.6, the non-dedicated ports, which display `false` in the `Is Dedicated?` column, also display `disabled` in the `State` column.

3. Configure the non-dedicated ports for storage use, on one of the controller modules:

   You must repeat the applicable command for each port you are configuring.

If your HA pair is running…	Then…
ONTAP 9.8 or later	`storage port modify -node node name -port port name -mode storage`
ONTAP 9.7 or 9.6	`storage port enable -node node name -port port name`

4. If your HA pair is running ONTAP 9.6, reboot the controller module so that the port changes take effect: `system node reboot -node node name -reason reason for the reboot`

   Otherwise, go to the next step.

   The reboot can take up to 15 minutes.

5. Repeat steps for the second controller module:

If your HA pair is running…	Then…
ONTAP 9.7 or later	a. Repeat step 3. b. Go to step 6.
ONTAP 9.6	a. Repeat steps 3 and 4. The first controller must have already completed its reboot. b. Go to step 6.

6. Verify that the non-dedicated ports on both controller modules are configured for storage use: `storage port show`

   You can enter the command on either controller module.

   If your HA pair is running ONTAP 9.8 or later, the non-dedicated ports display `storage` in the `Mode` column.

If your HA pair is running ONTAP 9.7 or 9.6, the non-dedicated ports, which display `false` in the `Is Dedicated?` column, also display `enabled` in the `State` column.

Prepare an AFF A700, AFF A800, or AFF A400 HA pair to hot-add a second shelf

If you have an AFF A700, AFF A800, or AFF A400 HA pair with one NS224 drive shelf that is cabled to one set of RoCE-capable ports on each controller, you must recable the shelf (after you have installed the additional RoCE-capable PCIe cards or I/O modules) across both sets of ports on each controller, before hot-adding the second shelf.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have enabled the ports on the RoCE-capable PCIe cards or I/O modules you installed.

  Prepare non-dedicated RoCE-capable ports for a hot-add

About this task

- Recabling port connections is a nondisruptive procedure when your shelf has multipath-HA connectivity.

  You recable the first shelf across both sets of ports on each controller so that when you hot-add the second shelf, both shelves have more resilient connectivity.

- You move one cable at a time to maintain connectivity to the shelf at all times during this procedure.

Steps

1. Recable the existing shelf's connections across both sets of ports on each controller, as applicable to your platform model.

   ⓘ Moving a cable does not require any wait time between unplugging the cable from one port and plugging it into another port.

If you have an…	Then…
AFF A700 HA pair	ⓘ The substeps assume the existing shelf is cabled to RoCE-capable I/O modules in slot 3 on each controller. ⓘ If needed, you can reference cabling illustrations showing an existing single shelf and the recabled shelf, in a two shelf configuration. Cable a hot-add shelf for an AFF A700 HA pair a. On controller A, move the cable from slot 3 port b (e3b) to slot 7 port b (e7b). b. Repeat the same cable move on controller B.

If you have an…	Then…
AFF A800 HA pair	The substeps assume the existing shelf is cabled to RoCE-capable PCIe cards in slot 5 on each controller. If needed, you can reference cabling illustrations showing an existing single shelf and the recabled shelf, in a two shelf configuration. Cable a hot-add shelf for an AFF A800 HA pair a. On controller A, move the cable from slot 5 port b (e5b) to slot 3 port b (e3b). b. Repeat the same cable move on controller B.
AFF A400 HA pair	If needed, you can reference cabling illustrations showing an existing single shelf and the recabled shelf, in a two shelf configuration. Cable a hot-add shelf for an AFF A400 HA pair a. On controller A, move the cable from port e0d to slot 5 Port b (e5b). b. Repeat the same cable move on controller B.

2. Verify that the recabled shelf is cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

Prepare to manually assign drive ownership for a hot-add

If you are manually assigning drive ownership for the NS224 drive shelf you are hot-adding, then you need to disable automatic drive assignment if it is enabled.

Before you begin

You must have met the system requirements.

Requirements for a hot-add

About this task

You need to manually assign drive ownership if drives in the shelf will be owned by both controller modules in the HA pair.

Steps

1. Verify whether automatic drive assignment is enabled: `storage disk option show`

   You can enter the command on either controller module.

   If automatic drive assignment is enabled, the output shows `on` in the `Auto Assign` column (for each

controller module).

2. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

   You must disable automatic drive assignment on both controller modules.

Install a drive shelf for a hot-add

Installing a new NS224 drive shelf involves installing the shelf into a rack or cabinet, connecting the power cords (which automatically powers on the shelf), and then setting the shelf ID.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

Steps

1. Install the rail-mount kit that came with your shelf by using the installation flyer that came in the kit box.

   Do not flange-mount the shelf.

2. Install and secure the shelf onto the support brackets and rack or cabinet by using the installation flyer.

   A fully loaded NS224 shelf can weigh up to 66.78 lbs (30.29 kg) and requires two people to lift or use of a hydraulic lift. Avoid removing shelf components (from the front or rear of the shelf) to reduce the shelf weight, because shelf weight will become unbalanced.

3. Connect the power cords to the shelf, secure them in with the power cord retainer, and then connect the power cords to different power sources for resiliency.

   A shelf powers up when connected to a power source; it does not have power switches. When functioning correctly, a power supply's bicolored LED illuminates green.

4. Set the shelf ID to a number that is unique within the HA pair:

   More detailed instructions are available:

   Change a shelf ID - NS224 shelves

   a. Remove the left end cap and locate the small hole to the right of the LEDs.
   b. Insert the end of a paper clip or similar tool into the small hole to reach the shelf ID button.
   c. Press and hold the button (for up to 15 seconds) until the first number on the digital display blinks, and then release the button.

> If the ID takes longer than 15 seconds to blink, press and hold the button again, making sure to press it in all the way.

d. Press and release the button to advance the number until you reach the desired number from 0 to 9.
e. Repeat substeps 4c and 4d to set the second number of the shelf ID.

   It can take up to three seconds (instead of 15 seconds) for the number to blink.

f. Press and hold the button until the second number stops blinking.

   After about five seconds, both numbers start blinking and the amber LED on the ODP illuminates.

g. Power-cycle the shelf to make the shelf ID take effect.

   You must unplug both power cords from the shelf, wait 10 seconds, and then plug them back in.

   When power is restored to the power supplies, their bicolored LEDs illuminate green.

Cable a drive shelf for a hot-add

You cable each NS224 drive shelf you are hot-adding so that each shelf has two connections to each controller module in the HA pair. Depending on the number of shelves you are hot-adding and your platform model, you use RoCE-capable ports on board the controllers, on RoCE-capable PCIe cards, a combination of both, or on RoCE-capable I/O modules.

Considerations when cabling for a hot-add

Familiarizing yourself with proper cable connector orientation, and the location and labeling of ports on the NS224 NSM drive shelf modules can be helpful before cabling your hot-added shelf.

- Cables are inserted with the connector pull-tab facing up.

  When a cable is inserted correctly, it clicks into place.

  After you connect both ends of the cable, the shelf and controller port LNK (green) LEDs illuminate. If a port LNK LED does not illuminate, reseat the cable.

- You can use the following illustration to help you physically identify the shelf NSM ports, e0a and e0b:

Cable a hot-add shelf for an AFF A900 HA pair

When additional storage is needed, you can hot-add up to three additional NS224 drive shelves (for a total of four shelves) to an AFF A900 HA pair.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

  Install a drive shelf for a hot-add

About this task

- This procedure assumes that your HA pair has at least one existing NS224 shelf and that you are hot-adding up to three additional shelves.
- If your HA pair has only one existing NS224 shelf, this procedure assumes that the shelf is cabled across two RoCE-capable 100GbE I/O modules on each controller.

Steps

1. If the NS224 shelf you are hot-adding will be the second NS224 shelf in the HA pair, complete the following substeps.

   Otherwise, go to the next step.

   a. Cable shelf NSM A port e0a to controller A slot 10 port a (e10a).
   b. Cable shelf NSM A port e0b to controller B slot 2 port b (e2b).
   c. Cable shelf NSM B port e0a to controller B slot 10 port a (e10a).
   d. Cable shelf NSM B port e0b to controller A slot 2 port b (e2b).

The following illustration shows the second shelf cabling (and the first shelf).

2. If the NS224 shelf you are hot-adding will be the third NS224 shelf in the HA pair, complete the following substeps.

   Otherwise, go to the next step.

   a. Cable shelf NSM A port e0a to controller A slot 1 port a (e1a).
   b. Cable shelf NSM A port e0b to controller B slot 11 port b (e11b).
   c. Cable shelf NSM B port e0a to controller B slot 1 port a (e1a).
   d. Cable shelf NSM B port e0b to controller A slot 11 port b (e11b).

      The following illustration shows the third shelf cabling.

AFF A900 HA pair with three NS224 shelves

3. If the NS224 shelf you are hot-adding will be the fourth NS224 shelf in the HA pair, complete the following substeps.

   Otherwise, go to the next step.

   a. Cable shelf NSM A port e0a to controller A slot 11 port a (e11a).
   b. Cable shelf NSM A port e0b to controller B slot 1 port b (e1b).
   c. Cable shelf NSM B port e0a to controller B slot 11 port a (e11a).
   d. Cable shelf NSM B port e0b to controller A slot 1 port b (e1b).

      The following illustration shows the fourth shelf cabling.

AFF A900 HA pair with four NS224 shelves

4. Verify that the hot-added shelf is cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

5. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then reenable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

Cable a hot-add shelf for a FAS500f, AFF A250, or ASA A250HA pair

When additional storage is needed, you can hot-add an NS224 drive shelf to a FAS500f, AFF A250, or ASA A250HA pair.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

  Install a drive shelf for a hot-add

About this task

When viewed from the rear of the platform chassis, the RoCE-capable card port on the left is port "a" (e1a) and the port on the right is port "b" (e1b).

Steps

1. Cable the shelf connections:
   a. Cable shelf NSM A port e0a to controller A slot 1 port a (e1a).
   b. Cable shelf NSM A port e0b to controller B slot 1 port b (e1b).
   c. Cable shelf NSM B port e0a to controller B slot 1 port a (e1a).
   d. Cable shelf NSM B port e0b to controller A slot 1 port b (e1b).

   The following illustration shows the shelf cabling when completed.

2. Verify that the hot-added shelf is cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

3. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then reenable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

Cable a hot-add shelf for an AFF A700 HA pair

How you cable an NS224 drive shelf in an AFF A700 HA pair, depends on the number of shelves you are hot-adding and the number of RoCE-capable port sets (one or two) you are using on the controller modules.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

  Install a drive shelf for a hot-add

Steps

1. If you are hot-adding one shelf using one set of RoCE-capable ports (one RoCE capable I/O module) on each controller module, and this is the only NS224 shelf in your HA pair, complete the following substeps.

   Otherwise, go to the next step.

   > This step assumes that you installed the RoCE-capable I/O module in slot 3, instead of slot 7, on each controller module.

   a. Cable shelf NSM A port e0a to controller A slot 3 port a.
   b. Cable shelf NSM A port e0b to controller B slot 3 port b.
   c. Cable shelf NSM B port e0a to controller B slot 3 port a.
   d. Cable shelf NSM B port e0b to controller A slot 3 port b.

      The following illustration shows cabling for one hot-added shelf using one RoCE-capable I/O module in each controller module:

AFF A700 HA pair with one NS224 shelf

2. If you are hot-adding one or two shelves using two sets of RoCE-capable ports (two RoCE-capable I/O modules) in each controller module, complete the applicable substeps.

Shelves	Cabling
Shelf 1	These substeps assume that you are beginning the cabling by cabling shelf port e0a to the RoCE-capable I/O module in slot 3, instead of slot 7. a. Cable NSM A port e0a to controller A slot 3 port a. b. Cable NSM A port e0b to controller B slot 7 port b. c. Cable NSM B port e0a to controller B slot 3 port a. d. Cable NSM B port e0b to controller A slot 7 port b. e. If you are hot-adding a second shelf, complete the “Shelf 2” substeps; otherwise, go to step 3.
Shelf 2	These substeps assume that you are beginning the cabling by cabling shelf port e0a to the RoCE-capable I/O module in slot 7, instead of slot 3 (which correlates with the cabling substeps for shelf 1). a. Cable NSM A port e0a to controller A slot 7 port a. b. Cable NSM A port e0b to controller B slot 3 port b. c. Cable NSM B port e0a to controller B slot 7 port a. d. Cable NSM B port e0b to controller A slot 3 port b. e. Go to step 3.

The following illustration shows cabling for the first and second hot-added shelves:

3. Verify that the hot-added shelf is cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

4. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then reenable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

Cable a hot-add shelf for an AFF A800 HA pair

How you cable an NS224 drive shelf in an AFF A800 HA pair depends on the number of shelves you are hot-adding and the number of RoCE-capable port sets (one or two) you are using on the controller modules.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

  Install a drive shelf for a hot-add

Steps

1. If you are hot-adding one shelf using one set of RoCE-capable ports (one RoCE-capable PCIe card) on each controller module, and this is the only NS224 shelf in your HA pair, complete the following substeps.

   Otherwise, go to the next step.

   > This step assumes you installed the RoCE-capable PCIe card in slot 5.

   a. Cable shelf NSM A port e0a to controller A slot 5 port a.
   b. Cable shelf NSM A port e0b to controller B slot 5 port b.
   c. Cable shelf NSM B port e0a to controller B slot 5 port a.
   d. Cable shelf NSM B port e0b to controller A slot 5 port b.

   The following illustration shows cabling for one hot-added shelf using one RoCE-capable PCIe card on each controller module:

2. If you are hot-adding one or two shelves using two sets of RoCE-capable ports (two RoCE-capable PCIe cards) on each controller module, complete the applicable substeps.

   > This step assumes you installed the RoCE-capable PCIe cards in slot 5 and slot 3.

Shelves	Cabling
Shelf 1	These substeps assume you are beginning the cabling by cabling shelf port e0a to the RoCE-capable PCIe card in slot 5, instead of slot 3. a. Cable NSM A port e0a to controller A slot 5 port a. b. Cable NSM A port e0b to controller B slot 3 port b. c. Cable NSM B port e0a to controller B slot 5 port a. d. Cable NSM B port e0b to controller A slot 3 port b. e. If you are hot-adding a second shelf, complete the “Shelf 2” substeps; otherwise, go to step 3.
Shelf 2	These substeps assume you are beginning the cabling by cabling shelf port e0a to the RoCE-capable PCIe card in slot 3, instead of slot 5 (which correlates with the cabling substeps for shelf 1). a. Cable NSM A port e0a to controller A slot 3 port a. b. Cable NSM A port e0b to controller B slot 5 port b. c. Cable NSM B port e0a to controller B slot 3 port a. d. Cable NSM B port e0b to controller A slot 5 port b. e. Go to step 3.

The following illustration shows cabling for two hot-added shelves:

3. Verify that the hot-added shelf is cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

4. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then reenable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

Cable a hot-add shelf for an AFF A400 HA pair

How you cable an NS224 drive shelf in an AFF A400 HA pair, depends on the number of shelves you are hot-adding and the number of RoCE-capable port sets (one or two) you are using on the controller modules.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

Install a drive shelf for a hot-add

Steps

1. If you are hot-adding one shelf using one set of RoCE-capable ports (onboard RoCE-capable ports) on each controller module, and this is the only NS224 shelf in your HA pair, complete the following substeps.

   Otherwise, go to the next step.

   a. Cable shelf NSM A port e0a to controller A port e0c.
   b. Cable shelf NSM A port e0b to controller B port e0d.
   c. Cable shelf NSM B port e0a to controller B port e0c.
   d. Cable shelf NSM B port e0b to controller A port e0d.

   The following illustration shows cabling for one hot-added shelf using one set of RoCE-capable ports on each controller module:

2. If you are hot-adding one or two shelves using two sets of RoCE-capable ports (on board and PCIe card RoCE-capable ports) on each controller module, complete the following substeps.

Shelves	Cabling
Shelf 1	a. Cable NSM A port e0a to controller A port e0c. b. Cable NSM A port e0b to controller B slot 5 port b. c. Cable NSM B port e0a to controller B port e0c. d. Cable NSM B port e0b to controller A slot 5 port b. e. If you are hot-adding a second shelf, complete the “Shelf 2” substeps; otherwise, go to step 3.

Shelves	Cabling
Shelf 2	a. Cable NSM A port e0a to controller A slot 5 port a. b. Cable NSM A port e0b to controller B port e0d. c. Cable NSM B port e0a to controller B slot 5 port a. d. Cable NSM B port e0b to controller A port e0d. e. Go to step 3.

The following illustration shows cabling for two hot-added shelves:

3. Verify that the hot-added shelf is cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

4. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then re enable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

Cable a hot-add shelf for an AFF A320 HA pair

You cable a second NS224 drive shelf to an existing HA pair when additional storage is needed.

Before you begin

- You must have met the system requirements.

Requirements for a hot-add

- You must have completed the applicable preparation procedures.

  Prepare for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

  Install a drive shelf for a hot-add

About this task

This procedure assumes that your AFF A320 HA pair has an existing NS224 shelf and that you are hot-adding a second shelf.

Steps

1. Cable the shelf to the controller modules.
   a. Cable NSM A port e0a to controller A port e0e.
   b. Cable NSM A port e0b to controller B port e0b.
   c. Cable NSM B port e0a to controller B port e0e.
   d. Cable NSM B port e0b to controller A port e0b.

   The following illustration shows cabling for the hot-added shelf (shelf 2):

2. Verify that the hot-added shelf is cabled correctly.

If any cabling errors are generated, follow the corrective actions provided.

NetApp Downloads: Config Advisor

3. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then re enable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

Complete the hot-add

If you disabled automatic drive assignment as part of the preparation for the NS224 drive shelf hot-add, you need to manually assign drive ownership and then reenable automatic drive assignment if needed.

Before you begin

You must have already cabled your shelf as instructed for your HA pair.

Cable a drive shelf for a hot-add

Steps

1. Display all unowned drives: `storage disk show -container-type unassigned`

   You can enter the command on either controller module.

2. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

   You can enter the command on either controller module.

   You can use the wild card character to assign more than one drive at once.

3. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

   You must reenable automatic drive assignment on both controller modules.

Change a shelf ID - NS224 shelves

You can change a shelf ID in a system when ONTAP is not yet running or when hot-adding a shelf prior to it being cabled to the system. You can also change a shelf ID when ONTAP is up and running (controller modules are available to serve data) and all drives in the shelf are unowned, spares, or part of offlined aggregate(s).

Before you begin

- If ONTAP is up and running (controller modules are available to serve data), you must have verified that all drives in the shelf are unowned, spares, or part of offlined aggregate(s).

  You can verify the state of the drives by using the `storage disk show -shelf` *`shelf_number`* command. Output in the `Container Type` column should display `spare` or `broken` if it is a failed drive. Additionally, the `Container Name` and `Owner` columns should have a dash.

- You need a paper clip with one side straightened or a narrow-tipped ballpoint pen.

  You use the paper clip or ballpoint pen to access the shelf ID button through the small hole, to the right of the LEDs, in the Operator Display Panel (ODP).

About this task

- A valid shelf ID is 00 through 99.
- Shelf IDs must be unique within an HA pair.
- You must power cycle a shelf (unplug both power cords, wait the appropriate amount of time, and then plug them back in) in order for the shelf ID to take effect.

  The amount of time you wait before plugging the power cords back in depends on the state of ONTAP, as described later in this procedure.

  NS224 shelves do not have power switches on the power supplies.

Steps

1. Power on the shelf, if it's not already on.

   You connect the power cords first to the shelf, securing them in place with the power cord retainer, and then connect the power cords to different power sources for resiliency.

2. Remove the left end cap to locate the small hole to the right of the LEDs.
3. Change the first number of the shelf ID:
   a. Insert the paper clip or ballpoint pen into the small hole.
   b. Press and hold the button until the first number on the digital display blinks, and then release the button.

      It can take up to 15 seconds for the number to blink. This activates the shelf ID programming mode.

      If the ID takes longer than 15 seconds to blink, press and hold the button again, making sure to press it in all the way.

   c. Press and release the button to advance the number until you reach the desired number from 0 to 9.

      Each press and release duration can be as short as one second.

      The first number continues to blink.

4. Change the second number of the shelf ID:
   a. Press and hold the button until the second number on the digital display blinks.

      It can take up to three seconds for the number to blink.

      The first number on the digital display stops blinking.

   b. Press and release the button to advance the number until you reach the desired number from 0 to 9.

      The second number continues to blink.

5. Lock in the desired number and exit the programming mode by pressing and holding the button until the second number stops blinking.

   It can take up to three seconds for the number to stop blinking.

   Both numbers on the digital display start blinking and the amber LED on the ODP illuminates after about five seconds, alerting you that the pending shelf ID has not yet taken effect.

6. Power-cycle the shelf to make the shelf ID take effect.

   You must unplug the power cord from both power supplies on the shelf, wait the appropriate amount of time, and then plug them back into the shelf power supplies to complete the power cycle.

   A power supply is powered on as soon as the power cord is plugged in. Its bicolored LED should illuminate green.

   - If ONTAP is not yet running or you are hot-adding a shelf (that has not yet been cabled to the system), wait at least 10 seconds.
   - If ONTAP is running (controllers are available to serve data), and all drives in the shelf are unowned, spares, or part of offlined aggregate(s), wait at least 70 seconds.

     This time allows ONTAP to properly delete the old shelf address and update the copy of the new shelf address.

7. Replace the left end cap.

Cable shelves as switch-attached storage - NS224 shelves

If you have a system in which the NS224 drive shelves need to be cabled as switch-attached storage (not direct-attached storage), use the information provided.

- Cable NS224 drive shelves through storage switches:

  Information for cabling switch-attached NS224 drive shelves

- Install your storage switches:

  AFF and FAS Switch Documentation

- Confirm supported hardware, such as storage switches and cables, for your platform model:

  NetApp Hardware Universe

Maintain

Replace the boot media - NS224 shelves

When the boot media fails on an NS224 drive shelf in an HA pair that is running ONTAP 9.7 or later, or the shelf is running NVMe shelf module (NSM) firmware version 1.1x or later, you can replace the boot media. Replacing the boot media can be done nondisruptively, while the drive shelf is powered on, and I/O is in progress.

Before you begin

- Your HA pair must already be running ONTAP 9.7 or later, which has the minimum supported version of NSM firmware, or your HA pair must already be running a version of ONTAP 9.6 with NSM firmware version 1.1x or later.

  You can enter the `storage shelf show -module` command at the console of either controller to verify the version of NSM firmware on your shelf.

  > If your shelf is not running NSM firmware version 1.1x or later, you cannot replace the boot media, you must replace the NSM module.
  >
  > Replace an NSM module - NS224 shelves

- You need a Phillips #1 screwdriver.

  The screw used to secure the boot media to the board requires a Phillips #1 screwdriver; using a different type of screwdriver could strip the screw.

- The shelf's partner NSM module must be up and running, and be cabled correctly so that your shelf maintains connectivity when you remove the NSM module with the failed FRU (target NSM module).

  NetApp Downloads: Config Advisor

- All other components in the system must be functioning properly.

About this task

- After the boot media is replaced, the boot image from the shelf's partner NSM module is automatically copied to the replacement boot media.

  This can take up to five minutes.

- Allow at least 70 seconds between removal and installation of the NVMe shelf module (NSM).

  This allows enough time for ONTAP to process the NSM removal event.

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

  If you do not know the *`shelf_name`* of the affected shelf, run the `storage shelf show` command.

  A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the `off` option.

- After replacing the boot media, you can return the failed part to NetApp as described in the RMA instructions shipped with the kit.

If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- You can use the following video or the written steps to replace the boot media.

  Replacing the boot media in an NS224 drive shelf

Steps

1. Properly ground yourself.
2. Disconnect the cabling from the NSM module that contains the FRU that you are replacing:
   a. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

      Power supplies do not have a power switch.

   b. Disconnect the storage cabling from the NSM module ports.

      Make a note of the NSM module ports that each cable is connected to. You reconnect the cables to the same ports when you reinsert the NSM module, later in this procedure.

3. Remove the NSM module from the shelf:
   a. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are removing the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   b. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

      The latching mechanisms raise, clearing the latching pins on the shelf.

   c. Gently pull until the NSM module is about one third of the way out of the shelf, grasp the NSM module sides with both hands to support its weight, and then place it on a flat stable surface.

      When you begin pulling, the latching mechanism arms extend from the NSM module and lock in their fully extended position.

4. Loosen the NSM module cover thumb screw and open the cover.
5. Physically locate the failed boot media.

   The boot media is located along the shelf chassis wall opposite from the power supply. The boot media attention (amber) LED, located on the board next to the boot media slot, is illuminated.

   > The LED remains illuminated for 10 minutes after you remove the NSM module from the shelf.

6. Replace the boot media:
   a. Using the Phillips #1 screwdriver, carefully remove the screw securing the bottom (notched) end of the boot media to the board.

b. Remove the boot media by rotating the notched end up slightly and then gently pulling it towards you until it releases from the socket.

   You can hold the boot media by placing your thumb and forefinger on the side edges, at the notched end.

c. Unpack the boot media from the antistatic bag.

d. Insert the replacement boot media by pushing it gently into the socket until it is seated squarely and completely in the socket.

   You can hold the boot media by placing your thumb and forefinger on the side edges, at the notched end. Make sure that the side with the heat sink is facing up.

   When correctly seated, and when you let go of the boot media, the notched end of the boot media is angled up, away from the board, because it is not yet secured with the screw.

e. Gently hold down the notched end of the boot media as you insert and tighten the screw with the screwdriver to secure the boot media in place.

   > Tighten the screw just enough to hold the boot media securely in place, but do not overtighten.

7. Close the NSM module cover, and then tighten the thumb screw.
8. Reinsert the NSM module into the shelf:
   a. Make sure that the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, gently slide the NSM module into the shelf until the weight of the NSM module is fully supported by the shelf.
   c. Push the NSM module into the shelf until it stops (about half an inch from the back of the shelf).

      You can place your thumbs on the orange tabs on the front of each finger loop (of the latching mechanism arms) to push in the NSM module.

   d. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are inserting the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   e. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.
   f. Gently push forward to get the latches over the stop.
   g. Release your thumbs from the tops of the latching mechanisms, and then continue pushing until the latching mechanisms snap into place.

      The NSM module should be fully inserted into the shelf and flush with the edges of the shelf.

9. Reconnect the cabling to the NSM module:
   a. Reconnect the storage cabling to the same two NSM module ports.

      Cables are inserted with the connector pull-tab facing up. When a cable is inserted correctly, it clicks

into place.

b. Reconnect the power cord to the power supply, and then secure the power cord with the power cord retainer.

   When functioning correctly, a power supply's bicolored LED illuminates green.

   Additionally, both NSM module port LNK (green) LEDs illuminate. If a LNK LED does not illuminate, reseat the cable.

10. Verify that the attention (amber) LEDs on the NSM module containing the failed boot media and the shelf operator display panel are no longer illuminated.

    It can take between 5 to 10 minutes for the attention LEDs to turn off. This is the amount of time it takes the NSM module to reboot and the boot media image copy to complete.

    If the fault LEDs remain on, the boot media might not be seated correctly or there might be another issue and you should contact technical support for assistance.

11. Verify that the NSM module is cabled correctly, by running Active IQ Config Advisor.

    If any cabling errors are generated, follow the corrective actions provided.

    NetApp Downloads: Config Advisor

Replace a DIMM - NS224 shelves

You can replace a faulty DIMM nondisruptively in an NS224 drive shelf that is powered on, and while I/O is in progress.

Before you begin

- The shelf's partner NSM module must be up and running, and be cabled correctly so that your shelf maintains connectivity when you remove the NSM module with the failed FRU (target NSM module).

  NetApp Downloads: Config Advisor

- All other components in the system, including the other three DIMMs, must be functioning properly.

About this task

- Allow at least 70 seconds between removal and installation of the NVMe shelf module (NSM).

  This allows enough time for ONTAP to process the NSM removal event.

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf:
  `storage shelf location-led modify -shelf-name shelf_name -led-status on`

If you do not know the *shelf_name* of the affected shelf, run the `storage shelf show` command.

A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the `off` option.

- When you unpack the replacement DIMM, save all packing materials for use when you return the failed DIMM.

  If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- You can use the following video or the written steps to replace a DIMM.

  Replacing a DIMM in an NS224 drive shelf

Steps

1. Properly ground yourself.
2. Disconnect the cabling from the NSM module that contains the FRU that you are replacing:
   a. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

      Power supplies do not have a power switch.

   b. Disconnect the storage cabling from the NSM module ports.

      Make a note of the NSM module ports that each cable is connected to. You reconnect the cables to the same ports when you reinsert the NSM module, later in this procedure.

3. Remove the NSM module from the shelf:
   a. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are removing the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   b. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

      The latching mechanisms raise, clearing the latching pins on the shelf.

   c. Gently pull until the NSM module is about one third of the way out of the shelf, grasp the NSM module sides with both hands to support its weight, and then place it on a flat stable surface.

      When you begin pulling, the latching mechanism arms extend from the NSM module and lock in their fully extended position.

4. Loosen the NSM module cover thumb screw and open the cover.

   The FRU label on the NSM module cover shows the location of the four DIMMs, two on either side of the heat sink, in the center of the NSM module.

5. Physically identify the faulty DIMM.

   When a DIMM is faulty, the system logs a warning message to the system console indicating which DIMM is faulty. Additionally, the DIMM attention (amber) LED, located on the board next to the DIMM slot, illuminates.

   > The LED for the faulty DIMM remains illuminated for 10 minutes after you remove the NSM module from the shelf.

6. Replace the faulty DIMM:
   a. Note the orientation of the DIMM in the slot so that you can insert the replacement DIMM using the same orientation.
   b. Eject the DIMM from its slot by slowly pushing apart the ejector tabs at both ends of the DIMM slot, and then lift the DIMM out of the slot.

      > Carefully hold the DIMM by the corners or edges to avoid pressure on the DIMM circuit board components.

      The ejector tabs remain in the open position.

   c. Remove the replacement DIMM from its antistatic shipping bag.
   d. Hold the DIMM by the corners, and then insert the DIMM squarely into a slot.

      The notch on the bottom of the DIMM, among the pins, should line up with the tab in the slot.

      When inserted correctly, the DIMM should go in easily but fit tightly in the slot. If not, reinsert the DIMM.

   e. Push down carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at both ends of the DIMM.
7. Close the NSM module cover, and then tighten the thumb screw.
8. Reinsert the NSM module into the shelf:
   a. Make sure that the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, gently slide the NSM module into the shelf until the weight of the NSM module is fully supported by the shelf.
   c. Push the NSM module into the shelf until it stops (about half an inch from the back of the shelf).

      You can place your thumbs on the orange tabs on the front of each finger loop (of the latching mechanism arms) to push in the NSM module.

   d. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are inserting the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   e. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.
   f. Gently push forward to get the latches over the stop.

g. Release your thumbs from the tops of the latching mechanisms, and then continue pushing until the latching mechanisms snap into place.

   The NSM module should be fully inserted into the shelf and flush with the edges of the shelf.

9. Reconnect the cabling to the NSM module:
   a. Reconnect the storage cabling to the same two NSM module ports.

      Cables are inserted with the connector pull-tab facing up. When a cable is inserted correctly, it clicks into place.

   b. Reconnect the power cord to the power supply, and then secure the power cord with the power cord retainer.

      When functioning correctly, a power supply's bicolored LED illuminates green.

      Additionally, both NSM module port LNK (green) LEDs illuminate. If a LNK LED does not illuminate, reseat the cable.

10. Verify that the attention (amber) LEDs on the NSM module containing the failed DIMM and the shelf operator display panel are no longer illuminated.

    The NSM module attention LEDs turn off after the NSM module reboots and no longer detects a DIMM issue. This can take three to five minutes.

11. Verify that the NSM module is cabled correctly, by running Active IQ Config Advisor.

    If any cabling errors are generated, follow the corrective actions provided.

    NetApp Downloads: Config Advisor

Hot-swap a drive - NS224 shelves

You can replace a failed drive nondisruptively in an NS224 drive shelf that is powered on, and while I/O is in progress.

Before you begin

- The drive that you are installing must be supported by the NS224 shelf.

  NetApp Hardware Universe

- If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP documentation.

  Instructions in the ONTAP documentation describe additional steps you must perform before and after replacing an SED.

  NetApp encryption overview with the CLI

- All other components in the system must be functioning properly; if not, contact technical support.
- Verify that the drive you are removing is failed.

  You can verify that the drive is failed by running the `storage disk show -broken` command. The

failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

> Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

About this task

- **Best practice:** The best practice is to have the current version of the Disk Qualification Package (DQP) installed before hot-swapping a drive.

  Having the current version of the DQP installed allows your system to recognize and use newly qualified drives. This avoids system event messages about having noncurrent drive information and prevention of drive partitioning because drives are not recognized. The DQP also notifies you of noncurrent drive firmware.

  NetApp Downloads: Disk Qualification Package

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- Drive firmware is automatically updated (nondisruptively) on new drives that have non-current firmware versions.

  > Drive firmware checks occur every two minutes.

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

  If you do not know the *`shelf_name`* of the affected shelf, run the `storage shelf show` command.

  A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the `off` option.

- When you unpack the replacement drive, save all packing materials for use when you return the failed drive.

  If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- The following video provides an overview of the physical removal and insertion portions of the drive hot-swap procedure.

  Hot-swapping a drive in an NS224 drive shelf

Steps

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment if it is enabled.

   > You need to manually assign drive ownership if drives in the shelf are owned by both controller modules in the HA pair.

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the `Auto Assign` column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive's activity (green) LED is illuminated.

When the drive's activity LED is solid, it means that the drive has power. When the drive's activity LED is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat steps 3 through step 7.
9. If you disabled automatic drive assignment in step 1, manually assign drive ownership, and then reenable automatic drive assignment if needed:
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

Replace a fan - NS224 shelves

You can replace a failed fan nondisruptively in an NS224 drive shelf that is powered on, and while I/O is in progress.

Before you begin

- The shelf's partner NSM module must be up and running, and be cabled correctly so that your shelf maintains connectivity when you remove the NSM module with the failed FRU (target NSM module).

  NetApp Downloads: Config Advisor

- All other components in the system, including the other four fans, must be functioning properly.

About this task

- Allow at least 70 seconds between removal and installation of the NVMe shelf module (NSM).

  This allows enough time for ONTAP to process the NSM removal event.

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

If you do not know the *shelf_name* of the affected shelf, run the `storage shelf show` command.

A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the `off` option.

- When you unpack the replacement fan, save all packing materials for use when you return the failed fan.

  If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- You can use the following video or the written steps to replace a fan.

  Replacing a fan in an NS224 drive shelf

Steps

1. Properly ground yourself.
2. Disconnect the cabling from the NSM module that contains the FRU that you are replacing:
   a. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

      Power supplies do not have a power switch.

   b. Disconnect the storage cabling from the NSM module ports.

      Make a note of the NSM module ports that each cable is connected to. You reconnect the cables to the same ports when you reinsert the NSM module, later in this procedure.

3. Remove the NSM module from the shelf:
   a. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are removing the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   b. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

      The latching mechanisms raise, clearing the latching pins on the shelf.

   c. Gently pull until the NSM module is about one third of the way out of the shelf, grasp the NSM module sides with both hands to support its weight, and then place it on a flat stable surface.

      When you begin pulling, the latching mechanism arms extend from the NSM module and lock in their fully extended position.

4. Loosen the NSM module cover thumb screw and open the cover.

   > The FRU label on the NSM module cover shows the location of the five fans, along the rear wall of the NSM module.

5. Physically identify the failed fan.

   When a fan fails, the system logs a warning message to the system console indicating which fan failed. Additionally, the fan attention (amber) LED, located on the board near the fan slot, illuminates.

   > The LED for the failed fan remains illuminated for 10 minutes after you remove the NSM module from the shelf.

6. Replace the failed fan:
   a. Remove the failed fan by firmly grasping the sides, where the blue touch points are located, and then lift it vertically to disconnect it from the socket.
   b. Insert the replacement fan by aligning it within the guides, and then push down until the fan module connector is fully seated in the socket.
7. Close the NSM module cover, and then tighten the thumb screw.
8. Reinsert the NSM module into the shelf:
   a. Make sure that the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, gently slide the NSM module into the shelf until the weight of the NSM module is fully supported by the shelf.
   c. Push the NSM module into the shelf until it stops (about half an inch from the back of the shelf).

      You can place your thumbs on the orange tabs on the front of each finger loop (of the latching mechanism arms) to push in the NSM module.

   d. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are inserting the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   e. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.
   f. Gently push forward to get the latches over the stop.
   g. Release your thumbs from the tops of the latching mechanisms, and then continue pushing until the latching mechanisms snap into place.

      The NSM module should be fully inserted into the shelf and flush with the edges of the shelf.

9. Reconnect the cabling to the NSM module:
   a. Reconnect the storage cabling to the same two NSM module ports.

      Cables are inserted with the connector pull-tab facing up. When a cable is inserted correctly, it clicks into place.

   b. Reconnect the power cord to the power supply, and then secure the power cord with the power cord retainer.

      When functioning correctly, a power supply's bicolored LED illuminates green.

      Additionally, both NSM module port LNK (green) LEDs illuminate. If a LNK LED does not illuminate,

reseat the cable.

10. Verify that the attention (amber) LEDs on the NSM module containing the failed fan and the shelf operator display panel are no longer illuminated.

    The NSM module attention LEDs turn off after the NSM module reboots and no longer detects a fan issue. This can take three to five minutes.

11. Verify that the NSM module is cabled correctly, by running Active IQ Config Advisor.

    If any cabling errors are generated, follow the corrective actions provided.

    NetApp Downloads: Config Advisor

Hot-remove a shelf - NS224 shelves

You can hot-remove an NS224 drive shelf that has had the aggregates removed from the drives, in an HA pair that is up and serving data (I/O is in progress).

Before you begin

- Your HA pair cannot be in a takeover state.
- You must have removed all aggregates from the drives (the drives must be spares) in the shelf you are removing.

  > If you attempt this procedure with aggregates on the shelf you are removing, you could fail the system with a multidisk panic.

  You can use the `storage aggregate offline -aggregate` *`aggregate_name`* command and then the `storage aggregate delete -aggregate` *`aggregate_name`* command.

- If your system shipped in a system cabinet, you need a Phillips screwdriver to remove the screws securing the shelf to the cabinet rear uprights.

About this task

- If you are hot-removing more than one shelf, you remove one shelf at a time.
- **Best practice:** The best practice is to remove drive ownership after you remove the aggregates from the drives in the shelf you are removing.

  Removing ownership information from a spare drive allows the drive to be properly integrated into another node (as needed).

  The procedure for removing ownership from drives can be found in the disks and aggregates content:

  Disks and aggregates overview

> The procedure requires you to disable automatic drive assignment. You reenable automatic drive assignment at the end of this procedure (after you have hot-removed the shelf).

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name` *`shelf_name`* `-led-status on`

If you do not know the *shelf_name* of the affected shelf, run the `storage shelf show` command.

A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

- After disconnecting a shelf from non-dedicated RoCE capable ports (on board the controllers, on RoCE capable PCIe cards, a combination of both, or on I/O modules), you have the option of reconfiguring these ports for networking use.

> If your HA pair is running a version of ONTAP 9.6, you need to reboot the controllers one at a time.
> If your HA pair is running ONTAP 9.7 or later, you do not need to reboot the controllers, unless one or both controllers are in maintenance mode. This procedure assumes that neither controller is in maintenance mode.

Steps

1. Properly ground yourself.
2. Verify that the drives in the shelf you are removing have no aggregates (are spares) and that ownership is removed:

   a. Enter the following command to list all of the drives in the shelf that you are removing: `storage disk show -shelf shelf_number`

      You can enter the command on either controller module.

   b. Check the output to verify that there are no aggregates on the drives.

      Drives with no aggregates have a dash in the `Container Name` column.

   c. Check the output to verify that ownership is removed from the drives.

      Drives with no ownership have a dash in the `Owner` column.

      > If you have failed drives, they display broken in the `Container Type` column. (Failed drives do not have ownership.)

      The following output shows drives on the shelf being removed (shelf 2) are in a correct state for removing the shelf. The aggregates are removed on all of the drives; therefore, a dash appears in the `Container Name` column for each drive. Ownership is also removed on all of the drives; therefore, a dash appears in the `Owner` column for each drive.

```
cluster1::> storage disk show -shelf 2

           Usable           Disk     Container   Container
Disk         Size Shelf Bay Type     Type        Name       Owner
-------- -------- ----- --- ------   ----------- ---------- ---------
...
2.2.4           -     2   4 SSD-NVM  spare                -         -
2.2.5           -     2   5 SSD-NVM  spare                -         -
2.2.6           -     2   6 SSD-NVM  broken               -         -
2.2.7           -     2   7 SSD-NVM  spare                -         -
...
```

3. Physically locate the shelf you are removing.
4. Disconnect the cabling from the shelf you are removing:
   a. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

      Power supplies do not have a power switch.

   b. Disconnect the storage cabling (from the shelf to the controllers).
5. Physically remove the shelf from the rack or cabinet.

   A fully loaded NS224 shelf can weigh up to 66.78 lbs (30.29 kg) and requires two people to lift or use of a hydraulic lift. Avoid removing shelf components (from the front or rear of the shelf) to reduce the shelf weight, because shelf weight will become unbalanced.

   If your system was shipped in a cabinet, you must first unscrew the two Phillips screws securing the shelf to the rear uprights. The screws are located on the inside shelf walls of the bottom NSM module. You should remove both NSM modules to access the screws.

6. If you are removing more than one shelf, repeat steps 2 through 5.

   Otherwise, go to the next step.

7. If you disabled automatic drive assignment when you removed ownership from the drives, reenable it: `storage disk option modify -autoassign on`

   You run the command on both controller modules.

8. You have the option of reconfiguring the non-dedicated RoCE capable ports for networking use, by completing the following substeps.

   Otherwise, you are done with this procedure.

   a. Verify the names of the non-dedicated ports, currently configured for storage use: `storage port show`

      You can enter the command on either controller module.

> The non-dedicated ports configured for storage use are displayed in the output as follows:
> If your HA pair is running ONTAP 9.8 or later, the non-dedicated ports display `storage` in the `Mode` column.
> If your HA pair is running ONTAP 9.7 or 9.6, the non-dedicated ports, which display `false` in the `Is Dedicated?` column, also display `enabled` in the `State` column.

b. Complete the set of steps applicable to the version of ONTAP your HA pair is running:

If your HA pair is running…	Then…
ONTAP 9.8 or later	a. Reconfigure the non-dedicated ports for networking use, on the first controller module: `storage port modify -node` *`node name`* `-port` *`port name`* `-mode network` You must run this command for each port you are reconfiguring. b. Repeat the above step to reconfigure the ports on the second controller module. c. Go to substep 8c to verify all port changes.
ONTAP 9.7	a. Reconfigure the non-dedicated ports for networking use, on the first controller module: `storage port disable -node` *`node name`* `-port` *`port name`* You must run this command for each port you are reconfiguring. b. Repeat the above step to reconfigure the ports on the second controller module. c. Go to substep 8c to verify all port changes.

If your HA pair is running…	Then…
A version of ONTAP 9.6	a. Reconfigure the RoCE capable ports for networking use, on the first controller module: `storage port disable -node` *`node name`* `-port` *`port name`* You must run this command for each port you are reconfiguring. b. Reboot the controller module to make the port changes take effect: `system node reboot -node` *`node name`* `-reason` *`reason`* `for the reboot` The reboot must complete before you proceed to the next step. The reboot can take up to 15 minutes. c. Reconfigure the ports on the second controller module, by repeating the first step (a). d. Reboot the second controller to make the port changes take effect, by repeating the second step (b). e. Go to substep 8c to verify all port changes.

c. Verify that the non-dedicated ports of both controller modules are reconfigured for networking use: `storage port show`

   You can enter the command on either controller module.

   If your HA pair is running ONTAP 9.8 or later, the non-dedicated ports display `network` in the `Mode` column.

   If your HA pair is running ONTAP 9.7 or 9.6, the non-dedicated ports, which display `false` in the `Is Dedicated?` column, also display `disabled` in the `State` column.

Replace an NSM module - NS224 shelves

You can replace an impaired NVMe shelf module (NSM) nondisruptively in an NS224 drive shelf that is powered on, and while I/O is in progress.

Before you begin

- The shelf's partner NSM module must be up and running, and be cabled correctly so that your shelf maintains connectivity when you remove the failed NSM module.

  NetApp Downloads: Config Advisor

- All other components in the system must be functioning properly.

About this task

- Replacing the NSM module involves moving the DIMMs, fans and power supply from the impaired NSM module to the replacement NSM module.

  You do not move the real-time clock (RTC) battery or boot media. They come preinstalled in the replacement NSM module.

- Allow at least 70 seconds between removal and installation of the NVMe shelf module (NSM).

  This allows enough time for ONTAP to process the NSM removal event.

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- Shelf (NSM) firmware is automatically updated (nondisruptively) on a new NSM module that has a non-current firmware version.

  NSM module firmware checks occur every 10 minutes. An NSM module firmware update can take up to 30 minutes.

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

  If you do not know the `shelf_name` of the affected shelf, run the `storage shelf show` command.

  A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the `off` option.

- When you unpack the replacement NSM module, save all packing materials for use when you return the failed NSM module.

  If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- You can use the following video or the written steps to replace an NSM module.

  Replacing an NSM module in an NS224 drive shelf

Steps

1. Properly ground yourself.
2. Physically identify the impaired NSM module.

   The system logs a warning message to the system console indicating which module is impaired. Additionally, the attention (amber) LED on the drive shelf operator display panel and the impaired module illuminate.

3. Disconnect the cabling from the impaired NSM module:
   a. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

      Power supplies do not have a power switch.

   b. Disconnect the storage cabling from the NSM module ports.

      Make a note of the NSM module ports that each cable is connected to. You reconnect the cables to the same ports on the replacement NSM module, later in this procedure.

4. Remove the NSM module from the shelf:
   a. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are removing the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   b. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

      The latching mechanisms raise, clearing the latching pins on the shelf.

   c. Gently pull until the NSM module is about one third of the way out of the shelf, grasp the NSM module sides with both hands to support its weight, and then place it on a flat stable surface.

      When you begin pulling, the latching mechanism arms extend from the NSM module and lock in their fully extended position.

5. Unpack the replacement NSM module, and set it on a level surface near the impaired NSM module.
6. Open the cover of the impaired NSM module and the replacement NSM module by loosening the thumbscrew on each cover.

   > The FRU label on the NSM module cover shows the location of the DIMMs and fans.

7. Move the DIMMs from the impaired NSM module to the replacement NSM module.
   a. Note the orientation of the DIMMs in the slots so that you can insert the DIMMs into the replacement NSM module using the same orientation.
   b. Eject a DIMM from its slot by slowly pushing apart the ejector tabs at both ends of the DIMM slot, and then lift the DIMM out of the slot.

      > Carefully hold the DIMM by the corners or edges to avoid pressure on the DIMM circuit board components.
      > The ejector tabs remain in the open position.

   c. Hold the DIMM by the corners, and then insert the DIMM squarely into a slot on the replacement NSM module.

      The notch on the bottom of the DIMM, among the pins, should line up with the tab in the slot.

      When inserted correctly, the DIMM should go in easily but fit tightly in the slot. If not, reinsert the DIMM.

d. Push down carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at both ends of the DIMM.

e. Repeat substeps 7a through 7d for the remaining DIMMs.

8. Move the fans from the impaired NSM module to the replacement NSM module.

   a. Firmly grasp a fan from the sides, where the blue touch points are located, and then lift it vertically to disconnect it from the socket.

      You might need to gently rock the fan back and forth to disconnect it before lifting it out.

   b. Align the fan with the guides in the replacement NSM module, and then push down until the fan module connector is fully seated in the socket.

   c. Repeat substeps 8a and 8b for the remaining fans.

9. Close the cover of each NSM module, and then tighten each thumbscrew.

10. Move the power supply from the impaired NSM module to the replacement NSM module.

    a. Rotate the cam handle to its open (horizontal) position, and then grasp it.

    b. With your thumb, press the blue tab to release the locking mechanism.

    c. Pull the power supply out of the NSM module while using your other hand to support its weight.

    d. Using both hands, support and align the edges of the power supply with the opening in the replacement NSM module.

    e. Gently push the power supply into the NSM module until the locking mechanism clicks into place.

       Do not use excessive force or you might damage the internal connector.

    f. Rotate the cam handle to the closed position.

11. Insert the replacement NSM module into the shelf:

    a. Make sure that the latching mechanism arms are locked in the fully extended position.

    b. Using both hands, gently slide the NSM module into the shelf until the weight of the NSM module is fully supported by the shelf.

    c. Push the NSM module into the shelf until it stops (about half an inch from the back of the shelf).

       You can place your thumbs on the orange tabs on the front of each finger loop (of the latching mechanism arms) to push in the NSM module.

    d. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

       If you are inserting the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

    e. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

    f. Gently push forward to get the latches over the stop.

    g. Release your thumbs from the tops of the latching mechanisms, and then continue pushing until the latching mechanisms snap into place.

       The NSM module should be fully inserted into the shelf and flush with the edges of the shelf.

12. Reconnect the cabling to the NSM module:
    a. Reconnect the storage cabling to the same two NSM module ports.

       Cables are inserted with the connector pull-tab facing up. When a cable is inserted correctly, it clicks into place.

    b. Reconnect the power cord to the power supply, and then secure the power cord with the power cord retainer.

       When functioning correctly, a power supply's bicolored LED illuminates green.

       Additionally, both NSM module port LNK (green) LEDs illuminate. If a LNK LED does not illuminate, reseat the cable.
13. Verify that the attention (amber) LED on the shelf operator display panel is no longer illuminated.

    The operator display panel attention LED turns off after the NSM module reboots. This can take three to five minutes.
14. Verify that the NSM module is cabled correctly, by running Active IQ Config Advisor.

    If any cabling errors are generated, follow the corrective actions provided.

    NetApp Downloads: Config Advisor

Hot-swap a power supply - NS224 shelves

You can replace a failed power supply nondisruptively in an NS224 drive shelf that is powered on, and while I/O is in progress.

About this task

- If you are replacing more than one power supply, you must do so one at a time so that the shelf maintains power.
- **Best practice:** The best practice is to replace the power supply within two minutes of removal from the NSM module.

  If you exceed the two minutes, the shelf continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.
- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

  If you do not know the `shelf_name` of the affected shelf, run the `storage shelf show` command.

A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

- When you unpack the replacement power supply, save all packing materials for use when you return the failed power supply.

  If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- You can use the following video or the written steps to replace a power supply.

  Hot-swapping a power supply in an NS224 drive shelf

Steps

1. Properly ground yourself.
2. Physically identify the failed power supply.

   The system logs a warning message to the system console indicating which power supply failed. Additionally, the attention (amber) LED on the shelf operator display panel illuminates and the bicolored LED on the failed power supply illuminates red.

3. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

   Power supplies do not have a power switch.

4. Remove the failed power supply:
   a. Rotate the cam handle to its open (horizontal) position, and then grasp it.
   b. With your thumb, press the blue tab to release the locking mechanism.
   c. Pull the power supply out of the NSM module while using your other hand to support its weight.
5. Insert the replacement power supply:
   a. Using both hands, support and align the edges of the power supply with the opening in the NSM module.
   b. Gently push the power supply into the NSM module until the locking mechanism clicks into place.

      Do not use excessive force or you might damage the internal connector.

   c. Rotate the cam handle to the closed position.
6. Connect the power cord to the power supply and secure the power cord with the power cord retainer.

   When functioning correctly, a power supply's bicolored LED illuminates green.

Replace the real-time clock battery - NS224 shelves

You can replace a failed real-time clock (RTC) battery nondisruptively in an NS224 drive shelf that is powered on, and while I/O is in progress.

Before you begin

- The shelf's partner NSM module must be up and running, and be cabled correctly so that your shelf maintains connectivity when you remove the NSM module with the failed FRU (target NSM module).

  NetApp Downloads: Config Advisor

- All other components in the system must be functioning properly.

About this task

- Allow at least 70 seconds between removal and installation of the NVMe shelf module (NSM).

  This allows enough time for ONTAP to process the NSM removal event.

- **Best practice:** The best practice is to have current versions of NVMe shelf module (NSM) firmware and drive firmware on your system before replacing FRU components.

  > Do not revert firmware to a version that does not support your shelf and its components.
  >
  > NetApp Downloads: Disk Shelf Firmware
  >
  > NetApp Downloads: Disk Drive Firmware

- If needed, you can turn on the shelf's location (blue) LEDs to aid in physically locating the affected shelf: `storage shelf location-led modify -shelf-name *shelf_name* -led-status on`

  If you do not know the `shelf_name` of the affected shelf, run the `storage shelf show` command.

  A shelf has three location LEDs: one on the operator display panel and one on each NSM module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the `off` option.

- When you unpack the replacement RTC battery, save all packing materials for use when you return the failed RTC battery.

  If you need the RMA number or additional help with the replacement procedure, contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific).

- You can use the following video or the written steps to replace an RTC battery.

  Replacing an RTC battery in an NS224 drive shelf

Steps

1. Properly ground yourself.
2. Disconnect the cabling from the NSM module that contains the FRU that you are replacing:
   a. Disconnect the power cord from the power supply by opening the power cord retainer, and then unplug the power cord from the power supply.

      Power supplies do not have a power switch.

   b. Disconnect the storage cabling from the NSM module ports.

      Make a note of the NSM module ports that each cable is connected to. You reconnect the cables to the

same ports when you reinsert the NSM module, later in this procedure.

3. Remove the NSM module from the shelf:
   a. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

      > If you are removing the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

   b. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

      The latching mechanisms raise, clearing the latching pins on the shelf.

   c. Gently pull until the NSM module is about one third of the way out of the shelf, grasp the NSM module sides with both hands to support its weight, and then place it on a flat stable surface.

      When you begin pulling, the latching mechanism arms extend from the NSM module and lock in their fully extended position.

4. Loosen the NSM module cover thumb screw and open the cover.

   The FRU label on the NSM module cover shows the location of the RTC battery, near the front of the NSM module and to the right of the power supply.

5. Physically identify the failed RTC battery.

   The RTC battery attention (amber) LED, located on the board next to the battery slot, illuminates.

   > The LED for the failed RTC battery remains illuminated for 10 minutes after you remove the NSM module from the shelf.

6. Replace the RTC battery:
   a. Remove the battery by gently pushing it away from the holder until it is at an inclined angle (tilted away from the holder), and then lift it out of the holder.
   b. Insert the replacement battery into the holder at an inclined angle (tilted away from the holder), push it into an upright position, and then press it firmly into the connector until it is fully seated.

      > The positive side of the battery, marked with a plus sign, is oriented outward (away from the holder), corresponding to the plus sign marked on the NSM module board.

7. Close the NSM module cover, and then tighten the thumb screw.
8. Reinsert the NSM module into the shelf:
   a. Make sure that the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, gently slide the NSM module into the shelf until the weight of the NSM module is fully supported by the shelf.
   c. Push the NSM module into the shelf until it stops (about half an inch from the back of the shelf).

      You can place your thumbs on the orange tabs on the front of each finger loop (of the latching mechanism arms) to push in the NSM module.

d. Loop your index fingers through the finger holes of the latching mechanisms on either side of the NSM module.

> If you are inserting the bottom NSM module, and if the bottom rail is obstructing access to the latching mechanisms, place your index fingers through the finger holes from the inside (by crossing your arms).

e. With your thumbs, press down and hold the orange tabs on top of the latching mechanisms.

f. Gently push forward to get the latches over the stop.

g. Release your thumbs from the tops of the latching mechanisms, and then continue pushing until the latching mechanisms snap into place.

   The NSM module should be fully inserted into the shelf and flush with the edges of the shelf.

9. Reconnect the cabling to the NSM module:

   a. Reconnect the storage cabling to the same two NSM module ports.

      Cables are inserted with the connector pull-tab facing up. When a cable is inserted correctly, it clicks into place.

   b. Reconnect the power cord to the power supply, and then secure the power cord with the power cord retainer.

      When functioning correctly, a power supply's bicolored LED illuminates green.

      Additionally, both NSM module port LNK (green) LEDs illuminate. If a LNK LED does not illuminate, reseat the cable.

10. Verify that the attention (amber) LEDs on the NSM module containing the failed RTC battery and the shelf operator display panel are no longer illuminated

    The NSM module attention LEDs turn off after the NSM module reboots and no longer detects an RTC battery issue. This can take three to five minutes.

11. Verify that the NSM module is cabled correctly, by running Active IQ Config Advisor.

    If any cabling errors are generated, follow the corrective actions provided.

    NetApp Downloads: Config Advisor

SAS shelves with IOM12 modules

Install and cable

Install and cable shelves for a new system installation - shelves with IOM12 modules

If your new system—HA pair or single-controller configuration—did not come installed in a cabinet, you can install and cable the disk shelves in a rack.

Requirements for installing and cabling disk shelves with IOM12 modules for a new system installation

You must meet certain requirements before installing and cabling the disk shelves.

- You must have the installation and setup instructions for your platform model.

  The installation and setup instructions address the complete procedure for your system installation, setup, and configuration. You only use this procedure (*Install and cable shelves for a new system installation*) in conjunction with the platform installation and setup instructions if you need detailed information about installing or cabling the disk shelves to your storage system.

  Installation and setup instructions can be found by navigating to your platform model documentation.

  AFF and FAS System Documentation

- Disk shelves and controllers must not be powered on at this time.
- If you are using mini-SAS HD SAS optical cables, you must have met the rules in Mini-SAS HD SAS optical cable rules.

Considerations for installing and cabling disk shelves with IOM12 modules for a new system installation

You should familiarize yourself with aspects and best practices about this procedure before installing and cabling the disk shelves.

General considerations

- Disk shelves with IOM12 modules are shipped with shelf IDs preset to 00.

  > If you have an HA pair with at least two stacks, the disk shelf containing the root aggregates for the second stack has the shelf ID preset to 10.

  You must set shelf IDs so they are unique within the HA pair or single-controller configuration. You can manually set shelf IDs or have shelf IDs automatically assigned for all disk shelves in the HA pair or single-controller configuration using a command in maintenance mode. Instructions for both methods are provided.

- Disk shelves containing the root aggregates can be identified by the labels on the disk shelf box and disk shelf chassis.

  The labels show the stack number; for example, "`Loop or Stack #: 1 `" and "`Loop or Stack #: 2 `". Disk shelves that do not contain the root aggregates only show the disk shelf serial number is on the labels.

- If at system setup and configuration, you do not configure the system to use automatic disk ownership assignment, you need to manually assign disk ownership.
- In-band Alternate Control Path (ACP) is automatically enabled.

  In-band ACP is not supported on single-path HA or single-path configurations.

Best practice considerations

- The best practice is to have the current version of the Disk Qualification Package (DQP) installed.

  Having the current version of the DQP installed allows your system to recognize and utilize newly qualified

disk drives; therefore, avoiding system event messages about having non-current disk drive information. You also avoid the possible prevention of disk partitioning because disk drives are not recognized. The DQP also notifies you of non-current disk drive firmware.

NetApp Downloads: Disk Qualification Package

- The best practice is to download and run Config Advisor after a new system installation.

  Running Config Advisor after a new system installation allows you to verify SAS connections are cabled correctly and that shelf IDs are unique within the HA pair or single-controller configuration.

  If any SAS cabling or duplicate shelf ID errors are generated, follow the corrective actions provided.

  You need network access to download Config Advisor.

  NetApp Downloads: Config Advisor

SAS cable handling considerations

- Visually inspect the SAS port to verify the proper orientation of the connector before plugging it in.

  The SAS cable connectors are keyed. When oriented correctly into a SAS port, the connector clicks into place and if the disk shelf power is on at the time, the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

  For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

- To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

  Cables have a minimum bend radius. Cable manufacturer specifications define the minimum bend radius; however, a general guideline for minimum bend radius is 10 times the cable diameter.

- Using Velcro wraps instead of tie-wraps to bundle and secure system cables allows for easier cable adjustments.

Install disk shelves with IOM12 modules for a new system installation

You install the disk shelves in a rack using the rack mount kits that came with the disk shelves.

1. Install the rack mount kit (for two-post or four-post rack installations) that came with your disk shelf using the installation flyer that came with the kit.

   If you are installing multiple disk shelves, you should install them from the bottom to the top of the rack for the best stability.

   Do not flange-mount the disk shelf into a telco-type rack; the disk shelf's weight can cause it to collapse in the rack under its own weight.

2. Install and secure the disk shelf onto the support brackets and rack using the installation flyer that came with the kit.

To make a disk shelf lighter and easier to maneuver, remove the power supplies and I/O modules (IOMs).

For DS460C disk shelves, you can also use the four detachable handles that shipped with your disk shelf. Handles (two on each side of the chassis) are installed by pushing up until they click into place. As you slide the disk shelf onto the rails, detach handles using the thumb latch.

It is recommended that you use a mechanical hoist or lift if you are moving a fully loaded DS460C disk shelf.

> A fully loaded DS460C disk shelf can weigh approximately 247 lbs (112 kg).

3. If you are installing a DS460C disk shelf, install the components into the racked disk shelf; otherwise, go to the next step.

   If you purchased a partially populated disk shelf which does not have a drive in every drive slot, you must ensure that:

   - The first four slots (0, 3, 6, and 9) are occupied in each drawer.

     This ensures proper airflow in the disk shelf.

   - In a shelf with 30 drives, the remaining ten drives are distributed evenly throughout the shelf in slots 1 and 10 of each drawer.
     The following illustration shows how the drives are numbered from 0 to 11 in each drive drawer within the shelf. Slots 0, 3, 6, 9, and, in a shelf containing 30 drives, slots 1 and 10 in each drawer must contain drives.

a. Reinstall any power supplies and IOMs you removed prior to installing your disk shelf into the rack.
b. Open the top drawer of the shelf.
c. Raise the cam handle on the drive to vertical.
d. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.

1	Raised button on the right side of the drive carrier

e. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.

f. Repeat the previous substeps for each drive in the drawer.

   You must be sure that slots 0, 3, 6, and 9 in each drawer contain drives.

g. Carefully push the drive drawer back into the enclosure.

Possible loss of data access: Never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

h. Close the drive drawer by pushing both levers towards the center.

i. Repeat these steps for each drawer in the disk shelf.

4. If you are adding multiple disk shelves, repeat this procedure for each disk shelf you are installing.

Do not power on the disk shelves at this time.

Cable disk shelves with IOM12 modules for a new system installation

You cable disk shelf SAS connections—shelf-to-shelf (as applicable) and controller-to-shelf—to establish storage connectivity for the system.

Before you begin

You must have met the requirements in Requirements for installing and cabling disk shelves with IOM12 modules for a new system installation and installed the disk shelves in the rack.

About this task

After you cable the disk shelves, you power them on, set the shelf IDs, and complete system setup and configuration.

Steps

1. Cable the shelf-to-shelf connections within each stack if the stack has more than one disk shelf; otherwise, go to the next step:

   For a detailed explanation and examples of shelf-to-shelf “standard” cabling and shelf-to-shelf “double-wide” cabling, see shelf-to-shelf connection rules.

If…	Then…
You are cabling a multipath HA, multipath, single-path HA, or single-path configuration	Cable the shelf-to-shelf connections as “standard” connectivity (using IOM ports 3 and 1): a. Beginning with the logical first shelf in the stack, connect IOM A port 3 to the next shelf’s IOM A port 1 until each IOM A in the stack is connected. b. Repeat substep a for IOM B. c. Repeat substeps a and b for each stack.
You are cabling a quad-path HA or quad-path configuration	Cable the shelf-to-shelf connections as “double-wide” connectivity: You cable the standard connectivity using IOM ports 3 and 1 and then the double-wide connectivity using IOM ports 4 and 2. a. Beginning with the logical first shelf in the stack, connect IOM A port 3 to the next shelf’s IOM A port 1 until each IOM A in the stack is connected. b. Beginning with the logical first shelf in the stack, connect IOM A port 4 to the next shelf’s IOM A port 2 until each IOM A in the stack is connected. c. Repeat substeps a and b for IOM B. d. Repeat substeps a through c for each stack.

2. Identify the controller SAS port pairs that you can use to cable the controller-to-stack connections.
   a. Check the controller-to-stack cabling worksheets and cabling examples to see whether a completed worksheet exists for your configuration.

      Controller-to-stack cabling worksheets and cabling examples for common AFF A200, AFF A220, FAS2600 series and FAS2700 configurations

      Controller-to-stack cabling worksheets and cabling examples for common multipath HA configurations

      Controller-to-stack cabling worksheet and cabling example for a quad-path HA configuration with two quad-port SAS HBAs

   b. The next step depends on whether a completed worksheet exists for your configuration:

If…	Then…
There is a completed worksheet for your configuration	Go to the next step. You use the existing completed worksheet.

If…	Then…
There is no completed worksheet for your configuration	Fill out the appropriate controller-to-stack cabling worksheet template: Controller-to-stack cabling worksheet template for multipathed connectivity Controller-to-stack cabling worksheet template for quad-pathed connectivity

3. Cable the controller-to-stack connections using the completed worksheet.

   If needed, instructions for how to read a worksheet to cable controller-to-stack connections are available:

   How to read a worksheet to cable controller-to-stack connections for multipathed connectivity

   How to read a worksheet to cable controller-to-stack connections for quad-pathed connectivity

4. Connect the power supplies for each disk shelf:
   a. Connect the power cords first to the disk shelves, securing them in place with the power cord retainer, and then connect the power cords to different power sources for resiliency.
   b. Turn on the power supplies for each disk shelf and wait for the disk drives to spin up.
5. Set the shelf IDs and complete system setup:

   You must set shelf IDs so they are unique within the HA pair or single-controller configuration, including the internal disk shelf in applicable systems.

If…	Then…
You are manually setting shelf IDs	a. Access the shelf ID button behind the left end cap. b. Change the shelf ID to a unique ID (00 through 99). c. Power-cycle the disk shelf to make the shelf ID take effect. Wait at least 10 seconds before turning the power back on to complete the power cycle. The shelf ID blinks and the operator display panel amber LED blinks until you power cycle the disk shelf. d. Power on the controllers and complete system setup and configuration as instructed by the installation and setup instructions for your platform model.

If…	Then…
You are automatically assigning all shelf IDs in your HA pair or single-controller configuration Shelf IDs are assigned in sequential order from 00-99. For systems with an internal disk shelf, shelf ID assignment begins with the internal disk shelf.	a. Power on the controllers. b. As the controllers start booting, press `Ctrl-C` to abort the AUTOBOOT process when you see the message `Starting AUTOBOOT press Ctrl-C to abort`. If you miss the prompt and the controllers boot to ONTAP, halt both controllers, and then boot both controllers to the boot menu by entering `boot_ontap menu` at their LOADER prompt. c. Boot one controller to Maintenance mode:`boot_ontap menu` You only need to assign shelf IDs on one controller. d. From the boot menu, select option 5 for Maintenance mode. e. Automatically assign shelf IDs: `sasadmin expander_set_shelf_id -a` f. Exit Maintenance mode:`halt` g. Bring up the system by entering the following command at the LOADER prompt of both controllers:`boot_ontap` Shelf IDs appear in disk shelf digital display windows. Before you boot the system, best practice is to take this opportunity to verify cabling is correct, a root aggregate is present, and run system-level diagnostics to identify any faulty components. h. Complete system setup and configuration as instructed by the installation and setup instructions for your platform model.

6. If as part of system set up and configuration, you did not enable disk ownership automatic assignment, manually assign disk ownership; otherwise, go to the next step:
   a. Display all unowned disks:`storage disk show -container-type unassigned`
   b. Assign each disk:`storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`*

You can use the wildcard character to assign more than one disk at once.

7. Download and run Config Advisor as instructed by the installation and setup instructions for your platform model to verify SAS connections are cabled correctly and there are no duplicate shelf IDs within the system.

   If any SAS cabling or duplicate shelf ID errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

   You can also run the `storage shelf show -fields shelf-id` command to see a list of shelf IDs already in use (and duplicates if present) in your system.

8. Verify that in-band ACP was automatically enabled. `storage shelf acp show`

   In the output, “in-band” is listed as “active” for each node.

Hot-add a shelf - shelves with IOM12 modules

You can hot-add one or more disk shelves with IOM12 modules to an existing stack of disk shelves with IOM12 modules or hot-add a stack of one or more disk shelves with IOM12 modules directly to a SAS HBA or an onboard SAS port on the controller.

About this task

You cannot use this procedure to mix a stack: hot-add a shelf with IOM12 modules to a stack of shelves that has IOM6 modules. If you need to mix a stack, use Hot-add IOM12 shelves to a stack of IOM6 shelves.

Requirements for hot-adding disk shelves with IOM12 modules

Your system must meet certain requirements before hot-adding disk shelves with IOM12 modules.

State of your system

- Your system and version of ONTAP must support the disk shelves you are hot-adding, including the IOMs, disk drives, and SAS cables.

  NetApp Hardware Universe

- Your system must have less than the maximum number of disk drives supported, by at least the number of disk shelves you plan to hot-add.

  You cannot have exceeded the maximum number of disk drives supported for your system after hot-adding disk shelves.

  NetApp Hardware Universe

- If you are hot-adding a stack of one or more disk shelves (directly to the platform controllers), your system must have enough available PCI SAS HBA or onboard SAS ports or a combination of both.

> If you need to install an additional PCI SAS HBA, the best practice is to use 12Gb SAS HBAs to keep controller-to-stack connectivity at 12Gbs for maximum performance.
>
> Using 6Gb SAS HBAs or a combination of 6Gb SAS HBAs and 12Gb SAS HBAs is supported; however, IOM12 module connections to 6Gb SAS HBAs are negotiated down to 6Gbs, resulting in lower performance.

- Your system cannot have any SAS cabling error messages.

  Download and run Config Advisor to verify that your SAS connections are cabled correctly.

  You must correct any cabling errors using the corrective actions provided by the error messages.

  NetApp Downloads: Config Advisor

Using mini-SAS HD SAS optical cables

- If you are using mini-SAS HD SAS optical cables or a mix of mini-SAS HD SAS optical cables and SAS copper cables in the stack of disk shelves, you must have met the rules in Mini-SAS HD SAS optical cable rules.
- If you are hot-adding a disk shelf with mini-SAS HD SAS optical cables to a stack of disk shelves that is connected with SAS copper cables, you can temporarily have both cable types in the stack.

  After hot-adding the disk shelf, you must replace the SAS copper cables for the rest of the shelf-to-shelf connections in the stack and the controller-to-stack connections so that the stack meets the rules in Mini-SAS HD SAS optical cable rules. This means that you must have ordered the appropriate number of mini-SAS HD SAS optical cables.

Considerations for hot-adding disk shelves with IOM12 modules

You should familiarize yourself with aspects and best practices about this procedure before hot-adding disk shelves.

General considerations

- If you are hot-adding a disk shelf with IOM12 modules to an existing stack (of disk shelves with IOM12 modules), you can hot-add the disk shelf to either end—the logical first or last disk shelf—of the stack.

  For single-path HA and single-path configurations, as applicable to AFF A200, AFF A220, FAS2600 series, and FAS2700 systems, you hot-add disk shelves to the end of the stack that does not have controller connections.

- Disk shelves with IOM12 modules must be in their own unique stack; they cannot be added to a stack that has shelves with IOM6 modules or IOM3 modules.

  This procedure does not address mixing a stack: hot-adding a shelf with IOM12 modules to a stack of shelves with IOM6 modules.

- A system can have multipathed and quad-pathed stacks of disk shelves with IOM12 modules.

  If you have an HA pair, ONTAP shows the system configuration as “multipath HA”. If you have a single-controller configuration, ONTAP shows the system configuration as “multipath”.

- This procedure assumes your configuration is using in-band ACP.

  For configurations that have in-band ACP enabled, in-band ACP is automatically enabled on hot-added disk shelves. For configurations in which in-band ACP is not enabled, hot-added disk shelves operate without any ACP functionality.

- Nondisruptive stack consolidation is not supported.

  You cannot use this procedure to hot-add disk shelves that were hot-removed from another stack in the same system when the system is powered on and serving data (I/O is in progress).

Best practice considerations

- The best practice is to have the current version of the Disk Qualification Package (DQP) installed before hot-adding a disk shelf.

  Having the current version of the DQP installed allows your system to recognize and utilize newly qualified disk drives; therefore, avoiding system event messages about having non-current disk drive information. You also avoid the possible prevention of disk partitioning because disk drives are not recognized. The DQP also notifies you of non-current disk drive firmware.

  NetApp Downloads: Disk Qualification Package

- The best practice is to run Config Advisor before and after hot-adding a disk shelf.

  Running Config Advisor before hot-adding a disk shelf provides a snapshot of the SAS connectivity, verifies disk shelf (IOM) firmware versions, and allows you to verify shelf IDs already in use on your system. Running Config Advisor after hot-adding a disk shelf allows you to verify SAS connections are cabled correctly and that shelf IDs are unique within the HA pair or single-controller configuration.

  If any SAS cabling or duplicate shelf ID errors are generated, follow the corrective actions provided.

  You need network access to download Config Advisor.

  NetApp Downloads: Config Advisor

- The best practice is to have the current versions of disk shelf (IOM) firmware and disk drive firmware on your system before adding new disk shelves, shelf FRU components, or SAS cables.

  Current versions of firmware can be found on the NetApp Support Site.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

SAS cable handling considerations

- Visually inspect the SAS port to verify the proper orientation of the connector before plugging it in.

  The SAS cable connectors are keyed. When oriented correctly into a SAS port, the connector clicks into place and if the disk shelf power is on at the time, the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

  For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the

correct orientation of the SAS cable connector varies.

- To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

  Cables have a minimum bend radius. Cable manufacturer specifications define the minimum bend radius; however, a general guideline for minimum bend radius is 10 times the cable diameter.

- Using Velcro wraps instead of tie-wraps to bundle and secure system cables allows for easier cable adjustments.

Installing disk shelves with IOM12 modules for a hot-add

For each disk shelf you are hot-adding, you install the disk shelf into a rack, connect the power cords, power on the disk shelf, and set the disk shelf ID before cabling the SAS connections.

Steps

1. Install the rack mount kit (for two-post or four-post rack installations) that came with your disk shelf using the installation flyer that came with the kit.

   If you are installing multiple disk shelves, you should install them from the bottom to the top of the rack for the best stability.

   Do not flange-mount the disk shelf into a telco-type rack; the disk shelf's weight can cause it to collapse in the rack under its own weight.

2. Install and secure the disk shelf onto the support brackets and rack using the installation flyer that came with the kit.

   To make a disk shelf lighter and easier to maneuver, remove the power supplies and I/O modules (IOMs).

   For DS460C disk shelves, you can also use the four detachable handles that shipped with your disk shelf. Handles (two on each side of the chassis) are installed by pushing up until they click into place. As you slide the disk shelf onto the rails, detach handles using the thumb latch.

   It is recommended that you use a mechanical hoist or lift if you are moving a fully loaded DS460C disk shelf.

   A fully loaded DS460C disk shelf can weigh approximately 247 lbs (112 kg).

3. If you are installing a DS460C disk shelf, install the components into the racked disk shelf; otherwise, go to the next step.

   If you purchased a partially populated disk shelf which does not have a drive in every drive slot, you must ensure that:

   - The first four slots (0, 3, 6, and 9) are occupied in each drawer.

     This ensures proper airflow in the disk shelf.

   - In a shelf with 30 drives, the remaining ten drives are distributed evenly throughout the shelf in slots 1 and 10 of each drawer.
     The following illustration shows how the drives are numbered from 0 to 11 in each drive drawer within the shelf. Slots 0, 3, 6, 9, and, in a shelf containing 30 drives, slots 1 and 10 in each drawer must contain drives.

   a. Reinstall any power supplies and IOMs you removed prior to installing your disk shelf into the rack.
   b. Open the top drawer of the shelf.
   c. Raise the cam handle on the drive to vertical.

d. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.

1	Raised button on the right side of the drive carrier

e. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.

f. Repeat the previous substeps for each drive in the drawer.

   You must be sure that slots 0, 3, 6, and 9 in each drawer contain drives.

g. Carefully push the drive drawer back into the enclosure.

Possible loss of data access: Never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

h. Close the drive drawer by pushing both levers towards the center.

i. Repeat these steps for each drawer in the disk shelf.

4. If you are adding multiple disk shelves, repeat the previous steps for each disk shelf you are installing.
5. Connect the power supplies for each disk shelf:
   a. Connect the power cords first to the disk shelves, securing them in place with the power cord retainer, and then connect the power cords to different power sources for resiliency.
   b. Turn on the power supplies for each disk shelf and wait for the disk drives to spin up.
6. Set the shelf ID for each disk shelf you are hot-adding to an ID that is unique within the HA pair or single-controller configuration.

   If you have a system with an internal disk shelf, shelf IDs must be unique across the internal disk shelf and externally attached disk shelves.

   You can use the following substeps to change shelf IDs, or for more detailed instructions, use Change a shelf ID.

   a. If needed, verify shelf IDs already in use by running Config Advisor.

      You can also run the `storage shelf show -fields shelf-id` command to see a list of shelf IDs already in use (and duplicates if present) in your system.

   b. Access the shelf ID button behind the left end cap.
   c. Change the shelf ID to a valid ID (00 through 99).
   d. Power-cycle the disk shelf to make the shelf ID take effect.

      Wait at least 10 seconds before turning the power back on to complete the power cycle.

      The shelf ID blinks and the operator display panel amber LED blinks until you power cycle the disk shelf.

   e. Repeat substeps a through d for each disk shelf you are hot-adding.

Cabling disk shelves with IOM12 modules for a hot-add

You cable the SAS connections—shelf-to-shelf and controller-to-stack—as applicable for hot-added disk shelves so they have connectivity to the system.

Before you begin

You must have met the requirements in Requirements for hot-adding disk shelves with IOM12 modules and installed, powered on, and set shelf IDs for each disk shelf as instructed in Installing disk shelves with IOM12 modules for a hot-add.

About this task

- For an explanation and examples of shelf-to-shelf “standard” cabling and shelf-to-shelf “double-wide” cabling, see Shelf-to-shelf SAS connection rules.
- For instructions about how to read a worksheet to cable controller-to-stack connections, see How to read a worksheet to cable controller-to-stack connections for multipathed connectivity or How to read a worksheet to cable controller-to-stack connections for quad-pathed connectivity.
- After you have cabled the hot-added disk shelves, ONTAP recognizes them: disk ownership is assigned if disk ownership automatic assignment is enabled; disk shelf (IOM) firmware and disk drive firmware should automatically update if needed; and if in-band ACP is enabled on your configuration, it is automatically enabled on the hot-added disk shelves.

  Firmware updates can take up to 30 minutes.

Steps

1. If you want to manually assign disk ownership for the disk shelves you are hot-adding, you need to disable disk ownership automatic assignment if it is enabled; otherwise, go to the next step.

   You need to manually assign disk ownership if disks in the stack are owned by both controllers in an HA pair.

   You disable disk ownership automatic assignment before cabling the hot-added disk shelves and then later, in step 7, you reenable it after cabling the hot-added disk shelves.

   a. Verify if disk ownership automatic assignment is enabled:`storage disk option show`

      If you have an HA pair, you can enter the command at the console of either controller.

      If disk ownership automatic assignment is enabled, the output shows “on” (for each controller) in the “Auto Assign” column.

   b. If disk ownership automatic assignment is enabled, you need to disable it:`storage disk option modify -node _node_nam_e -autoassign off`

      You need to disable disk ownership automatic assignment on both controllers in an HA pair.

2. If you are hot-adding a stack of disk shelves directly to a controller, complete the following substeps; otherwise, go to step 3.

   a. If the stack you are hot-adding has more than one disk shelf, cable the shelf-to-shelf connections; otherwise, go to substep b.

If…	Then…
You are cabling a stack with multipath HA, multipath, single-path HA, or single-path connectivity to the controllers	Cable the shelf-to-shelf connections as “standard” connectivity (using IOM ports 3 and 1): i. Beginning with the logical first shelf in the stack, connect IOM A port 3 to the next shelf’s IOM A port 1 until each IOM A in the stack is connected. ii. Repeat substep i for IOM B.
You are cabling a stack with quad-path HA or quad-path connectivity to the controllers	Cable the shelf-to-shelf connections as “double-wide” connectivity: You cable the standard connectivity using IOM ports 3 and 1 and then the double-wide connectivity using IOM ports 4 and 2. i. Beginning with the logical first shelf in the stack, connect IOM A port 3 to the next shelf’s IOM A port 1 until each IOM A in the stack is connected. ii. Beginning with the logical first shelf in the stack, connect IOM A port 4 to the next shelf’s IOM A port 2 until each IOM A in the stack is connected. iii. Repeat substeps i and ii for IOM B.

b. Check the controller-to-stack cabling worksheets and cabling examples to see whether a completed worksheet exists for your configuration.

   Controller-to-stack cabling worksheets and cabling examples for common AFF A200, AFF A220, FAS2600 series and FAS2700 configurations

   Controller-to-stack cabling worksheets and cabling examples for common multipath HA configurations

   Controller-to-stack cabling worksheet and cabling example for a quad-path HA configuration with two quad-port SAS HBAs

c. If there is a completed worksheet for your configuration, cable the controller-to-stack connections using the completed worksheet; otherwise, go to the next substep.

d. If there is no completed worksheet for your configuration, fill out the appropriate worksheet template, and then cable the controller-to-stack connections using the completed worksheet.

   Controller-to-stack cabling worksheet template for multipathed connectivity

   Controller-to-stack cabling worksheet template for quad-pathed connectivity

e. Verify that all cables are securely fastened.

3. If you are hot-adding one or more disk shelves to an end—the logical first or last disk shelf—of an existing stack, complete the applicable substeps for your configuration; otherwise, go to the next step.

If you are…	Then…
Hot-adding a disk shelf to an end of a stack that has multipath HA, multipath, quad-path HA, or quad-path connectivity to the controllers	a. Disconnect any cables from IOM A of the disk shelf at the end of the stack that are connected to any controllers; otherwise, go to substep e. Leave the other end of these cables connected to the controllers, or replace cables with longer cables if needed. b. Cable the shelf-to-shelf connection(s) between IOM A of the disk shelf at the end of the stack and IOM A of the disk shelf you are hot-adding. c. Reconnect any cables that you removed in substep a to the same port(s) on IOM A of the disk shelf you are hot-adding; otherwise, go to the next substep. d. Verify that all cables are securely fastened. e. Repeat substeps a through d for IOM B; otherwise, go to Step 4.
Hot-adding a disk shelf to an end of the stack in a single-path HA or single-path configuration, as applicable to AFF A200, AFF A220, FAS2600 series and FAS2700 systems. These instructions are for hot-adding to the end of the stack that does not have controller-to-stack connections.	a. Cable the shelf-to-shelf connection between IOM A of the disk shelf in the stack and IOM A of the disk shelf you are hot-adding. b. Verify that the cable is securely fastened. c. Repeat applicable substeps for IOM B.

4. If you hot-added a disk shelf with mini-SAS HD SAS optical cables to a stack of disk shelves connected with SAS copper cables, replace the SAS copper cables; otherwise, go to the next step.

   The stack must meet the requirements stated in the Requirements for hot-adding disk shelves with IOM12 modules section of this procedure.

5. Download and run Config Advisor to verify that your SAS connections are cabled correctly.

   NetApp Downloads: Config Advisor

   If any SAS cabling errors are generated, follow the corrective actions provided.

6. Verify SAS connectivity for each hot-added disk shelf: `storage shelf show -shelf shelf_name -connectivity`

   You must run this command for each disk shelf you hot-added.

   For example, the following output shows hot-added disk shelf 2.5 is connected to initiator ports 1a and 0d (port pair 1a/0d) on each controller (in a FAS8080 multipath HA configuration with one quad-port SAS HBA):

```
cluster1::> storage shelf show -shelf 2.5 -connectivity

           Shelf Name: 2.5
             Stack ID: 2
             Shelf ID: 5
            Shelf UID: 40:0a:09:70:02:2a:2b
        Serial Number: 101033373
          Module Type: IOM12
                Model: DS224C
         Shelf Vendor: NETAPP
           Disk Count: 24
      Connection Type: SAS
          Shelf State: Online
               Status: Normal

Paths:

Controller     Initiator   Initiator Side Switch Port   Target Side
Switch Port   Target Port   TPGN
------------   ---------   --------------------------
-----------------------   -----------   ------
stor-8080-1    1a           -                           -
-             -
stor-8080-1    0d           -                           -
-             -
stor-8080-2    1a           -                           -
-             -
stor-8080-2    0d           -                           -
-             -

Errors:
------
-
```

7. If you disabled disk ownership automatic assignment in Step 1, manually assign disk ownership, and then reenable disk ownership automatic assignment if needed:
   a. Display all unowned disks:`storage disk show -container-type unassigned`
   b. Assign each disk:`storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`*

      You can use the wildcard character to assign more than one disk at once.

   c. Reenable disk ownership automatic assignment if needed:`storage disk option modify -node` *`node_name`* `-autoassign on`

      You need to reenable disk ownership automatic assignment on both controllers in an HA pair.

8. If your configuration is running in-band ACP, verify that in-band ACP was automatically enabled on hot-added disk shelves: `storage shelf acp show`

   In the output, “in-band” is listed as “active” for each node.

Hot-add IOM12 shelves to a stack of IOM6 shelves

When additional storage is needed, you can hot-add IOM12 shelves (SAS shelves with IOM12 modules) to a stack of IOM6 shelves (SAS shelves with IOM6 modules), meaning you can mix a stack.

Requirements for a hot-add

Your HA pair, single-controller or stretch MetroCluster configuration (system) must meet certain requirements before hot-adding IOM12 shelves to a stack of IOM6 shelves.

> For bridge-attached MetroCluster configurations, see Requirements for a hot-add in bridge-attached MetroCluster configurations.

- Your system and version of ONTAP must support a mix of IOM6 shelves and IOM12 shelves in the same stack (a mixed stack).

  You can verify support by using one of the following methods:

  - Enter the `run local sysconfig` command, at the admin prompt of either controller.

    If the SAS2/SAS3 Mixed Stack Support field does not appear in the output or has a value of none, then your system does not support mixed stacks.

    If anything else appears in the SAS2/SAS3 Mixed Stack Support field, such as all or bridge-attached, then your system does support mixed stacks.

  - Go to Hardware Universe and navigate to your platform information.

    NetApp Hardware Universe

- If you are adding a shelf to a MetroCluster configuration, the configuration must meet all requirements in the MetroCluster Installation and Configuration Guides.

  MetroCluster IP Installation and Configuration Guide

  ONTAP 9 Stretch MetroCluster Installation and Configuration Guide

  ONTAP 9 Fabric-attached MetroCluster Installation and Configuration Guide

- The stack of IOM6 shelves, to which you are hot-adding an IOM12 shelf, must be cabled with SAS copper cables (for all shelf-to-shelf and controller-to-stack connections).

  SAS optical cables are not supported in a mixed stack.

  > If the IOM6 shelf stack is cabled with any SAS optical cables, you cannot hot-add an IOM12 shelf. Contact your NetApp sales representative.

- Your system must have less than the maximum number of drives supported, by at least the number of drives capable of being installed in the IOM12 shelves you are hot-adding.

  You cannot have exceeded the maximum number of drives supported for your system after hot-adding IOM12 shelves.

  NetApp Hardware Universe

- Your system cannot have any SAS cabling error messages.

  You must correct any cabling errors using the corrective actions provided by the error messages.

  NetApp Downloads: Config Advisor

- You must have ordered and received the IOM12 shelves and appropriate number and types of SAS copper cables.

  IOM12 shelves use mini-SAS HD connectors. IOM6 shelves use QSFP connectors.

Requirements for a hot-add in bridge-attached MetroCluster configurations

If you are hot-adding IOM12 shelves to a stack of IOM6 shelves that is attached using a pair of ATTO FibreBridge bridges in a MetroCluster configuration, the system must meet certain requirements.

- If bridge SAS ports are available in the current configuration, you should add the IOM12 shelves as a separate stack.

  Use all bridge ports before mixing IOM12 and IOM6 modules in a stack.

- Your system and version of ONTAP must support a mix of IOM6 shelves and IOM12 shelves in the same stack (a mixed stack).

  You can verify support by using one of the following methods:

  - Enter the `run local sysconfig` command at the admin prompt of either controller.

    If the SAS2/SAS3 Mixed Stack Support field does not appear in the output or has a value of none, then your system does not support mixed stacks.

    If anything else appears in the SAS2/SAS3 Mixed Stack Support field, such as all or bridge-attached, then your system does support mixed stacks.

  - Go to Hardware Universe and navigate to your platform information.

    NetApp Hardware Universe

- The configuration must meet all requirements in the MetroCluster Installation and Configuration Guides.

  Installing and Configuring a Stretch MetroCluster Configuration

  Installing and Configuring a fabric-attached MetroCluster Configuration

- The stack of IOM6 shelves, to which you are hot-adding an IOM12 shelf, must be cabled with SAS copper cables (for all shelf-to-shelf and controller-to-stack connections).

SAS optical cables are not supported in a mixed stack.

> If the IOM6 shelf stack is cabled with any SAS optical cables, you cannot hot-add an IOM12 shelf. Contact your NetApp sales representative.

- Your configuration must have less than the maximum number of drives supported for a bridge port.
- You must have ordered and received the IOM12 shelves and appropriate number and types of SAS copper cables.

  IOM12 shelves use mini-SAS HD connectors. IOM6 shelves use QSFP connectors.

- The bridge must be running firmware version 3.16/4.16 and later.

Considerations for a hot-add

You should familiarize yourself with aspects and best practices about this procedure before hot-adding IOM12 shelves to a stack of IOM6 shelves.

General considerations

- It is highly recommended that the IOM12 shelves you are hot-adding are running firmware version 0260 or later, before you cable them to your system.

  Having a supported version of shelf firmware protects against storage stack access issues if you cabled the hot-added shelf to the stack incorrectly.

  After you download the IOM12 shelf firmware to your shelves, verify the firmware version is 0260 or later by entering the `storage shelf show -module` command at the console of either controller.

- Nondisruptive stack consolidation is not supported.

  You cannot use this procedure to hot-add disk shelves that were hot-removed from another stack in the same system when the system is powered on and serving data (I/O is in progress).

- You can use this procedure to hot-add disk shelves that were hot-removed within the same MetroCluster system if the affected shelf has mirrored aggregates.
- After you have cabled a hot-added shelf, ONTAP recognizes the shelf:
  - Drive ownership is assigned if automatic drive assignment is enabled.
  - Shelf (IOM) firmware and drive firmware should be updated automatically, if needed.

    > Firmware updates can take up to 30 minutes.

Best practice considerations

- **Best practice:** The best practice is to have current versions of shelf (IOM) firmware and drive firmware on your system before hot-adding a shelf.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

Do not revert firmware to a version that does not support your shelf and its components.

- **Best practice:** The best practice is to have the current version of the Disk Qualification Package (DQP) installed before hot-adding a shelf.

  Having the current version of the DQP installed allows your system to recognize and use newly qualified drives. This avoids system event messages about having noncurrent drive information and prevention of drive partitioning because drives are not recognized. The DQP also notifies you of noncurrent drive firmware.

  NetApp Downloads: Disk Qualification Package

- **Best practice:** The best practice is to run Active IQ Config Advisor before and after hot-adding a shelf.

  Running Active IQ Config Advisor before hot-adding a shelf provides a snapshot of the existing SAS connectivity, verifies shelf (IOM) firmware versions, and allows you to verify a shelf ID already in use on your system. Running Active IQ Config Advisor after hot-adding a shelf allows you to verify shelves are cabled correctly and that shelf IDs are unique within your system.

  NetApp Downloads: Config Advisor

- **Best practice:** The best practice is to have in-band ACP (IBACP) running on your system.
  - For systems in which IBAP is running, IBACP is automatically enabled on hot-added IOM12 shelves.
  - For systems in which out-of-band ACP is enabled, ACP capabilities are not available on IOM12 shelves.

    You should migrate to IBACP and remove the out-of-band ACP cabling.

  - If your system is not running IBACP, and your system meets the requirements for IBACP, you can migrate your system to IBACP before hot-adding an IOM12 shelf.

    Instructions for migrating to IBACP

    The migration instructions provide the system requirements for IBACP.

Prepare to manually assign drive ownership for a hot-add

If you are manually assigning drive ownership for the IOM12 shelves you are hot-adding, then you need to disable automatic drive assignment if it is enabled.

Before you begin

You must have met the system requirements.

Requirements for a hot-add

Requirements for a hot-add in bridge-attached MetroCluster configurations

About this task

If you have an HA pair, you need to manually assign drive ownership if drives in the shelf will be owned by both controller modules.

Steps

1. Verify whether automatic drive assignment is enabled: `storage disk option show`

   If you have an HA pair, you can enter the command on either controller module.

   If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

2. If automatic drive assignment is enabled, disable it: `storage disk option modify -node` *`node_name`* `-autoassign off`

   If you have an HA pair or two-node MetroCluster configuration, you must disable automatic drive assignment on both controller modules.

Install shelves for a hot-add

For each shelf you are hot-adding, you install the shelf into a rack, connect the power cords, power on the shelf, and set the shelf ID.

1. Install the rack mount kit (for two-post or four-post rack installations) that came with your disk shelf using the installation flyer that came with the kit.

   > If you are installing multiple disk shelves, you should install them from the bottom to the top of the rack for the best stability.

   > Do not flange-mount the disk shelf into a telco-type rack; the disk shelf’s weight can cause it to collapse in the rack under its own weight.

2. Install and secure the disk shelf onto the support brackets and rack using the installation flyer that came with the kit.

   To make a disk shelf lighter and easier to maneuver, remove the power supplies and I/O modules (IOMs).

   For DS460C disk shelves, you can also use the four detachable handles that shipped with your disk shelf. Handles (two on each side of the chassis) are installed by pushing up until they click into place. As you slide the disk shelf onto the rails, detach handles using the thumb latch.

   It is recommended that you use a mechanical hoist or lift if you are moving a fully loaded DS460C disk shelf.

   > A fully loaded DS460C disk shelf can weigh approximately 247 lbs (112 kg).

3. If you are installing a DS460C disk shelf, install the components into the racked disk shelf; otherwise, go to the next step.

   If you purchased a partially populated disk shelf which does not have a drive in every drive slot, you must ensure that:

   - The first four slots (0, 3, 6, and 9) are occupied in each drawer.

     This ensures proper airflow in the disk shelf.

   - In a shelf with 30 drives, the remaining ten drives are distributed evenly throughout the shelf in slots 1 and 10 of each drawer.

     The following illustration shows how the drives are numbered from 0 to 11 in each drive drawer within the shelf. Slots 0, 3, 6, 9, and, in a shelf containing 30 drives, slots 1 and 10 in each drawer must contain drives.

   a. Reinstall any power supplies and IOMs you removed prior to installing your disk shelf into the rack.
   b. Open the top drawer of the shelf.
   c. Raise the cam handle on the drive to vertical.

d. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.

1	Raised button on the right side of the drive carrier

e. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.

f. Repeat the previous substeps for each drive in the drawer.

   You must be sure that slots 0, 3, 6, and 9 in each drawer contain drives.

g. Carefully push the drive drawer back into the enclosure.

Possible loss of data access: Never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

h. Close the drive drawer by pushing both levers towards the center.

i. Repeat these steps for each drawer in the disk shelf.

4. If you are adding multiple disk shelves, repeat the previous steps for each disk shelf you are installing.
5. Connect the power supplies for each disk shelf:
   a. Connect the power cords first to the disk shelves, securing them in place with the power cord retainer, and then connect the power cords to different power sources for resiliency.
   b. Turn on the power supplies for each disk shelf and wait for the disk drives to spin up.
6. Set the shelf ID for each shelf you are hot-adding to an ID that is unique within the HA pair or single-controller configuration.

   A valid shelf ID is 00 through 99. It is recommended that you set the shelf IDs so that IOM6 shelves use lower numbers (1 - 9) and IOM12 shelves use higher numbers (10 and greater).

   If you have a platform model with onboard storage, shelf IDs must be unique across the internal shelf and externally attached shelves. It is recommended that you set the internal shelf to 0. In MetroCluster IP configurations, only the external shelf names apply, and therefore the shelf names do not need to be unique.

   a. If needed, verify shelf IDs already in use by running Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

      You can also run the `storage shelf show -fields shelf-id` command to see a list of shelf IDs already in use (and duplicates if present) in your system.

   b. Access the shelf ID button behind the left end cap.
   c. Change the first number of the shelf ID by pressing and holding the orange button until the first number on the digital display blinks, which can take up to three seconds.
   d. Press the button to advance the number until you reach the desired number.
   e. Repeat substeps c and d for the second number.
   f. Exit the programming mode by pressing and holding the button until the second number stops blinking, which can take up to three seconds.

g. Power cycle the shelf to make the shelf ID take effect.

   You must turn off both power switches, wait 10 seconds, and then turn them back on to complete the power cycle.

h. Repeat substeps b through g for each shelf you are hot-adding.

Cable shelves for a hot-add

How you cable an IOM12 shelf to a stack of IOM6 shelves depends on whether the IOM12 shelf is the initial IOM12 shelf, meaning no other IOM12 shelf exists in the stack, or whether it is an additional IOM12 shelf to an existing mixed stack, meaning one or more IOM12 shelves already exists in the stack. It also depends on whether the stack has multipath HA, multipath, single-path HA, or single-path connectivity.

Before you begin

- You must have met the system requirements.

  Requirements for a hot-add

- You must have completed the preparation procedure, if applicable.

  Prepare to manually assign drive ownership for a hot-add

- You must have installed the shelves, powered them on, and set the shelf IDs.

  Install shelves for a hot-add

About this task

- You always hot-add IOM12 shelves to the logical last shelf in a stack to maintain a single speed transition within the stack.

  By hot-adding IOM12 shelves to the logical last shelf in a stack, the IOM6 shelves remain grouped together and the IOM12 shelves remain grouped together so that there is a single speed transition between the two groups of shelves.

  For example:

  - In an HA pair, a single speed transition within a stack having two IOM6 shelves and two IOM12 shelves is depicted as:

    ```
    Controller <-> IOM6 <-> IOM6 <---> IOM12 <-> IOM12 <-> Controller
    ```

  - In an HA pair with onboard IOM12E storage, a single speed transition within a stack having two IOM12 shelves and two IOM6 shelves is depicted as:

    ```
    IOM12E 0b <-> IOM12 <-> IOM12 <---> IOM6 <-> IOM6 <-> IOM12E 0a
    ```

    The onboard storage port 0b is the port from the internal storage (expander) and because it connects to the hot-added IOM12 shelf (the last shelf in the stack), the group of IOM12 shelves is kept together

and a single transition is maintained through the stack and onboard IOM12E storage.

- Only a single speed transition is supported in a mixed stack. You cannot have additional speed transitions. For example, you cannot have two speed transitions within a stack, which is depicted as:

```
Controller <-> IOM6 <-> IOM6 <---> IOM12 <-> IOM12 <---> IOM6 <->
Controller
```

- You can hot-add IOM6 shelves to a mixed stack. However, you must hot-add them to the side of the stack with the IOM6 shelves (existing group of IOM6 shelves) in order to maintain the single speed transition in the stack.
- You cable IOM12 shelves by connecting the SAS ports on the IOM A path first, and then repeat the cabling steps for the IOM B path, as applicable to your stack connectivity.

  In a MetroCluster configuration, you cannot use the IOM B path.

- The initial IOM12 shelf (the IOM12 shelf connecting to the logical last IOM6 shelf) always connects to the IOM6 shelf circle ports (not square ports).
- The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place.

  For shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector). For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

- You can reference the following illustration for cabling IOM12 shelves to an IOM6 shelf stack in a configuration that is not using FC-to-SAS bridges.

  This illustration is specific to a stack with multipath HA connectivity; however, the cabling concept can be applied to stacks with multipath, single-path HA, single-path connectivity, and stretch MetroCluster configurations.

- You can reference the following illustration for cabling IOM12 shelves to an IOM6 shelf stack in a bridge-attached MetroCluster configuration.

Steps

1. Physically identify the logical last shelf in the stack.

   Depending on your platform model and stack connectivity (multipath HA, multipath, single-path HA, or single-path), the logical last shelf is the shelf having controller-to-stack connections from controller SAS ports B and D, or it is the shelf having no connections to any controllers (because the controller-to-stack connectivity is to the logical top of the stack, through the controller SAS ports A and C).

2. If the IOM12 shelf you are hot-adding is the initial IOM12 shelf being added to the IOM6 stack, meaning no other IOM12 shelf exists in the IOM6 shelf stack, complete the applicable substeps.

   Otherwise, go to step 3.

If your IOM6 stack connectivity is…	Then…
Multipath HA or multipath, or single-path HA with controller connectivity to the logical last shelf (including stretch MetroCluster configurations)	a. Disconnect the controller-to-stack cable from the last IOM6 shelf IOM A circle port to the controller or bridge. Make note of the controller port. Put the cable aside. It is no longer needed. Otherwise; go to substep e. b. Cable the shelf-to-shelf connection between the last IOM6 shelf IOM A circle port (from substep a) to the new IOM12 shelf IOM A port 1. Use a SAS copper QSFP-to-Mini-SAS HD cable. c. If you are hot-adding another IOM12 shelf, cable the shelf-to-shelf connection between the IOM12 shelf IOM A port 3, of the shelf you just cabled, and the next IOM12 shelf IOM A port 1. Use a SAS copper Mini-SAS HD-to-Mini-SAS HD cable. Otherwise, go to the next substep. d. Reestablish the controller-to-stack connection by cabling the same port on the controller or bridge (in substep a) to the new last IOM12 shelf IOM A port 3. Use a SAS copper QSFP-to-Mini-SAS HD cable or Mini-SAS HD-to-Mini-SAS HD cable, as appropriate for the port type on the controller. e. Repeat substeps a through d for IOM B. Otherwise, go to step 4.

If your IOM6 stack connectivity is…	Then…
Bridge-attached connectivity in a MetroCluster configuration	a. Disconnect the bottom bridge-to-stack cable from the last IOM6 shelf IOM A circle port to the bridge. Make note of the bridge port. Put the cable aside. It is no longer needed. Otherwise; go to substep e. b. Cable the shelf-to-shelf connection between the last IOM6 shelf IOM A circle port (from substep a) to the new IOM12 shelf IOM A port 1. Use a SAS copper QSFP-to-Mini-SAS HD cable. c. If you are hot-adding another IOM12 shelf, cable the shelf-to-shelf connection between the IOM12 shelf IOM A port 3, of the shelf you just cabled, and the next IOM12 shelf IOM A port 1. Use a SAS copper Mini-SAS HD-to-Mini-SAS HD cable. Otherwise, go to the next substep. d. Repeat substeps b and c to cable the shelf-to-shelf connections for IOM B. e. Reestablish the bottom bridge-to-stack connection by cabling the same port on the bridge (in substep a) to the new last IOM12 shelf IOM A port 3. Use a SAS copper QSFP-to-Mini-SAS HD cable or Mini-SAS HD-to-Mini-SAS HD cable, as appropriate for the port type on the controller. f. Go to step 4.

If your IOM6 stack connectivity is…	Then…
Single-path HA or single-path with no controller connectivity to the logical last shelf	a. Cable the shelf-to-shelf connection between the last IOM6 shelf IOM A circle port and the new IOM12 shelf IOM A port 1. Use a SAS copper QSFP-to-Mini-SAS HD cable. b. Repeat the above substep for IOM B. c. If you are hot-adding another IOM12 shelf, repeat substeps a and b. Otherwise, go to step 4.

3. If the IOM12 shelf you are hot-adding is an additional IOM12 shelf to an existing mixed stack, meaning one or more IOM12 shelves already exists in the stack, complete the applicable substeps.

If your mixed stack connectivity is…	Then…
Multipath HA or multipath, or single-path HA with controller connectivity to the logical last shelf, or bridge-attached connectivity in a MetroCluster configuration	a. Move the controller-to-stack cable from the last IOM12 shelf IOM A port 3 to the same port on the new last IOM12 shelf. b. If you are hot-adding one IOM12 shelf, cable the shelf-to-shelf connection between the old last IOM12 shelf IOM A port 3 to the new last IOM12 shelf IOM A port 1. Use a SAS copper Mini-SAS HD-to-Mini-SAS HD cable. Otherwise, go to the next substep. c. If you are hot-adding more than one IOM12 shelf, cable the shelf-to-shelf connection between the old last IOM12 shelf IOM A port 3 and the next IOM12 shelf IOM A port 1, and then repeat this for any additional IOM12 shelves. Use additional SAS copper Mini-SAS HD-to-Mini-SAS HD cables. Otherwise, go to the next substep. d. Repeat substeps a through c for IOM B. Otherwise, go to step 4.

If your mixed stack connectivity is…	Then…
Bridge-attached connectivity in a MetroCluster configuration	a. Move the bottom bridge-to-stack cable from the old last IOM12 shelf to the same port on the new last IOM12 shelf. b. Cable the shelf-to-shelf connection between the old last IOM12 shelf IOM A port 3 and the next IOM12 shelf IOM A port 1, and then repeat this for any additional IOM12 shelves. Use a SAS copper Mini-SAS HD-to-Mini-SAS HD cable. c. Cable the shelf-to-shelf connection between the old last IOM12 shelf IOM B port 3 and the next IOM12 shelf IOM B port 1, and then repeat this for any additional IOM12 shelves. d. Go to step 4.
Single-path HA or single-path with no controller connectivity to the logical last shelf	a. Cable the shelf-to-shelf connection between the last IOM12 shelf IOM A port 3 and the new last IOM12 shelf IOM A port 1. Use a SAS copper Mini-SAS HD-to-Mini-SAS HD cable. b. Repeat the above substep for IOM B. c. If you are hot-adding another IOM12 shelf, repeat substeps a and b. Otherwise, go to step 4.

4. Verify that the SAS connections are cabled correctly.

   If any cabling errors are generated, follow the corrective actions provided.

   NetApp Downloads: Config Advisor

5. If you disabled automatic drive assignment as part of the preparation for this procedure, you need to manually assign drive ownership and then re-enable automatic drive assignment, if needed.

   Otherwise, you are done with this procedure.

   Complete the hot-add

   All MetroCluster configurations require manual drive assignment.

Complete the hot-add

If you disabled automatic drive assignment as part of the preparation for hot-adding the IOM12 shelves to the stack of IOM6 shelves, you need to manually assign drive

ownership and then reenable automatic drive assignment if needed.

Before you begin

You must have already cabled your shelf as instructed for your system.

Cable shelves for a hot-add

Steps

1. Display all unowned drives: `storage disk show -container-type unassigned`

   If you have an HA pair, you can enter the command on either controller module.

2. Assign each drive: `storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`*

   If you have an HA pair, you can enter the command on either controller module.

   You can use the wild card character to assign more than one drive at once.

3. Reenable automatic drive assignment if needed: `storage disk option modify -node` *`node_name`* `-autoassign on`

   If you have an HA pair, you must reenable automatic drive assignment on both controller modules.

Change a shelf ID - shelves with IOM12 modules

You can change a shelf ID in a system when ONTAP is not yet running or when hot-adding a shelf prior to it being cabled to the system. You can also change a shelf ID when ONTAP is up and running (controller modules are available to serve data) and all drives in the shelf are unowned, spares, or part of offlined aggregate(s).

Before you begin

- If ONTAP is up and running (controller modules are available to serve data), you must have verified that all drives in the shelf are unowned, spares, or part of offlined aggregate(s).

  You can verify the state of the drives by using the `storage disk show -shelf` *`shelf_number`* command. Output in the Container Type column should display spare or broken if it is a failed drive. Additionally, the Container Name and Owner columns should have a dash.

- You can verify shelf IDs already in use in your system by running Active IQ Config Advisor or using the `storage shelf show -fields shelf-id` command.

  NetApp Downloads: Config Advisor

About this task

- A valid shelf ID is 00 through 99.
- Shelf IDs must be unique within an HA pair or single-controller configuration.

  If you have a platform with internal storage, shelf IDs must be unique across the internal disk shelf and any externally attached disk shelves.

- You must power cycle a shelf in order for the shelf ID to take effect.

The amount of time you wait before turning the power back on depends on the state of ONTAP, as described later in this procedure.

Steps

1. Turn on the power to the disk shelf if it is not already on.
2. Remove the left end cap to locate the button near the shelf LEDs.
3. Change the first number of the shelf ID by pressing and holding the orange button until the first number on the digital display blinks, which can take up to three seconds.

   > If the ID takes longer than three seconds to blink, press the button again, making sure to press it in all the way.
   >
   > This activates the disk shelf ID programming mode.

4. Press the button to advance the number until you reach the desired number from 0 to 9.

   The first number continues to blink.

5. Change the second number of the shelf ID by pressing and holding the button until the second number on the digital display blinks, which can take up to three seconds.

   The first number on the digital display stops blinking.

6. Press the button to advance the number until you reach the desired number from 1 to 9.

   The second number continues to blink.

7. Lock in the desired number and exit the programming mode by pressing and holding the button until the second number stops blinking, which can take up to three seconds.

   Both numbers on the digital display start blinking and the amber LED on the operator display panel illuminates after about five seconds, alerting you that the pending disk shelf ID has not yet taken effect.

8. Power cycle the disk shelf to make the shelf ID take effect.

   You must turn off both power switches, wait the appropriate amount of time, and then turn them back on to complete the power cycle.

   - If ONTAP is not yet running or you are hot-adding a shelf (that has not yet been cabled to the system), wait at least 10 seconds.
   - If ONTAP is running (controllers are available to serve data), and all disk drives in the shelf are unowned, spares, or part of offlined aggregate(s), wait at least 70 seconds.

     This time allows ONTAP to properly delete the old shelf address and update the copy of the new shelf address.

9. Replace the left end cap.
10. Repeat steps 1 through 9 for each additional disk shelf.
11. Verify that your system does not have duplicate shelf IDs.

    When two or more disk shelves have the same ID, the system assigns the duplicate disk shelf a soft ID number equal to or greater than 100. You must change the soft ID (duplicate) number.

a. Run Active IQ Config Advisor to check for duplicate shelf ID alerts or run the `storage shelf show -fields shelf-id` command to see a list of shelf IDs already in use including any duplicate IDs.

b. If your system has any duplicate shelf IDs, change the duplicate shelf IDs by repeating this procedure.

SAS cabling rules, worksheets, and examples

SAS cabling rules, worksheets, and examples overview - shelves with IOM12 modules

To help you cable your SAS drive shelves with IOM12 modules to your storage system, you can use any of the available SAS cabling rules, worksheets, and examples content as needed.

SAS cabling rules

- Configurations
- Controller slot numbering
- Shelf-to-shelf connections
- Controller-to-stack connections
- Mini-SAS HD SAS optical cables

Cabling worksheets and examples

- Common multipath HA configurations
- Common AFF A200, AFF A220, FAS2600, and FAS2700 configurations
- Quad-path HA configurations

Cabling worksheet templates

- Multipathed connectivity
- Quad-pathed connectivity
- How to read a worksheet for multipathed connectivity
- How to read a worksheet for quad-pathed connectivity

SAS cabling rules - shelves with IOM12 modules

Disk shelves with IOM12 modules can be cabled in HA pair and single-controller configurations (for supported platforms) by applying the SAS cabling rules: configuration rules, controller slot numbering rules, shelf-to-shelf connection rules, controller-to-stack connection rules, and if applicable, mini-SAS HD SAS optical cable rules.

> The SAS cabling rules regarding controller slot numbering rules, shelf-to-shelf connection rules, and controller-to-stack connection rules described in this guide are the same rules that apply to all SAS disk shelves, whether they have IOM12, IOM6, or IOM3 modules. However, the information in this guide is specific to the unique characteristics of disk shelves with IOM12 modules and their use in supported configurations.

The SAS cabling rules regarding configuration rules and mini-SAS HD SAS optical cable rules described in this guide are specific to disk shelves with IOM12 modules.

The SAS cabling rules described in this guide balance SAS cabling between the on-board SAS ports and host bus adapter SAS ports to provide highly available storage controller configurations and meet the following goals:

- Provide a single, easily understood universal algorithm for all SAS products and configurations
- Yield the same physical cabling when generating the Bill of Materials (BOM), followed in the factory, and in the field
- Are verifiable by configuration-checking software and tools
- Provide maximum possible resilience to maintain availability and minimize the reliance on controller takeovers

You should avoid deviating from the rules; deviations might reduce reliability, universality, and commonality.

Configuration rules

Disk shelves with IOM12 modules are supported in specific types of HA pair and single-controller configurations.

- HA pair configurations must be cabled as multipath HA or quad-path HA configurations with the following exceptions:
  - AFF A200, AFF A220, FAS2600 series and FAS2700HA pair configurations (with external disk shelves) can be cabled as single-path HA configurations to support connectivity to an external SAS tape backup device.
  - AFF A200, AFF A220, FAS2600 series and FAS2700HA pair configurations do not support quad-path HA connectivity.
- Single-controller configurations must be cabled as multipath or quad-path configurations, with the following exceptions:
  - FAS2600 series single-controller configurations (with external disk shelves) can be cabled as single-path configurations.

    Because the internal storage uses single-path connectivity, ONTAP issues occasional warnings that mixed paths are detected. To avoid these warnings, you can use single-path connectivity to the external disk shelves. Additionally, you can use single-path connectivity when an external SAS tape backup device is used.

  - FAS2600 series single-controller configurations do not support quad-path connectivity.

Controller slot numbering rules

For the purpose of applying cabling rules across all supported HA pairs and single-controller configurations, a controller slot numbering convention is used.

- For all HA pairs and single-controller configurations, the following applies:
  - A SAS HBA in a physical PCI slot is defined as occupying PCI slot 1, 2, 3, and so on regardless of the slot's physical label on a controller.

    For example, if SAS HBAs occupied physical PCI slots 3, 5, and 7, they would be designated as slots 1, 2, and 3 for the purpose of applying the SAS cabling rules.

  - An onboard SAS HBA is defined as occupying PCI slot 0 just as it is labeled on a controller.

- Each port in each slot is defined just as it is labeled on a controller.
  For example, slot 0 with two ports is referred to as 0a and 0b. Slot 1 with four ports is referred to as 1a, 1b, 1c, and 1d.

  In this document, slots and the slot ports are depicted as follows:

Shelf-to-shelf connection rules

When you have more than one disk shelf in a stack of disk shelves, they connect to each other through each SAS domain (IOM A and IOM B) using the applicable “standard” or “double-wide” shelf-to-shelf cabling. Your use of “standard” or “double-wide” shelf-to-shelf cabling depends on the configuration you have.

Standard shelf-to-shelf connectivity

- Standard shelf-to-shelf connectivity is used in multipath HA, multipath, single-path HA, and single-path configurations.
- Standard shelf-to-shelf connectivity is what is being used in existing SAS storage configurations with IOM3 and IOM6 modules: one cable connection is needed between disk shelves in each domain—domain A (IOM A) and domain B (IOM B).
- Best practice is to use IOM ports 3 and 1 for standard shelf-to-shelf connectivity.

  From the logical first shelf to the logical last shelf in a stack, you connect IOM port 3 to the next shelf’s IOM port 1 in domain A and then domain B.

Double-wide shelf-to-shelf connectivity

- Double-wide shelf-to-shelf connectivity is used in quad-pathed (quad-path HA and quad-path) configurations.
- Double-wide shelf-to-shelf connectivity requires two cable connections between disk shelves in each domain—domain A (IOM A) and domain B (IOM B).

  The first cable connection is cabled as standard shelf-to-shelf connectivity (using IOM ports 3 and 1); the second cable connection is cabled as double-wide shelf-to-shelf connectivity (using IOM ports 4 and 2).

  From the logical first shelf to the logical last shelf in a stack, you connect IOM port 3 to the next shelf's IOM port 1 in domain A and then domain B. From the logical first shelf to the logical last shelf in a stack, you connect IOM port 4 to the next shelf's IOM port 2 in domain A and then domain B. (IOM ports cabled as double-wide connectivity are shown with blue.)

Controller-to-stack connection rules

You can correctly cable the SAS connections from each controller to each stack in an HA pair or in a single-controller configuration by understanding that SAS disk shelves use software-based disk ownership, how controller ports A/C and B/D are connected to stacks, how controller ports A/C and B/D are organized into port pairs, and how AFF A200, AFF A220, FAS2600 series and FAS2700 system ports 0b and 0a are connected to stacks.

SAS disk shelf software-based disk ownership rule

SAS disk shelves use software-based disk ownership (not hardware-based disk ownership). This means that disk drive ownership is stored on the disk drive rather than it being determined by the topology of the storage system's physical connections (as it is for hardware-based disk ownership). Specifically, disk drive ownership is assigned by ONTAP (automatically or by CLI commands), not by how you cable the controller-to-stack connections.

SAS disk shelves should never be cabled using the hardware-based disk ownership scheme.

Controller A and C port connection rules (for non AFF A200, AFF A220, FAS2600 series and FAS2700 configurations)

- A and C ports are always the primary paths to a stack.
- A and C ports always connect to the logical first disk shelf in a stack.
- A and C ports always connect to disk shelf IOM ports 1 and 2.

  IOM port 2 is only used for quad-path HA and quad-path configurations.

- Controller 1 A and C ports always connect to IOM A (domain A).
- Controller 2 A and C ports always connect to IOM B (domain B).

The following illustration highlights how controller ports A and C connect in a multipath HA configuration with one quad-port HBA and two stacks of disk shelves. Connections to stack 1 are shown in blue. Connections to stack 2 are shown in orange.

Controller B and D port connection rules (for non AFF A200, AFF A220, FAS2600 series and FAS2700 configurations)

- B and D ports are always the secondary paths to a stack.
- B and D ports always connect to the logical last disk shelf in a stack.
- B and D ports always connect to disk shelf IOM ports 3 and 4.

  IOM port 4 is only used for quad-path HA and quad-path configurations.

- Controller 1 B and D ports always connect to IOM B (domain B).
- Controller 2 B and D ports always connect to IOM A (domain A).
- B and D ports are connected to the stacks by offsetting the order of the PCI slots by one so that the first port on the first slot is cabled last.

The following illustration highlights how controller ports B and D connect in a multipath HA configuration with one quad-port HBA and two stacks of disk shelves. Connections to stack 1 are shown in blue. Connections to stack 2 are shown in orange.

Port pair connection rules (for non AFF A200, AFF A220, FAS2600 series and FAS2700 configurations)

Controller SAS ports A, B, C, and D are organized into port pairs using a method that leverages all of the SAS ports for system resiliency and consistency when cabling controller-to-stack connections in HA pair and single-controller configurations.

- Port pairs consist of a controller A or C SAS port and a controller B or D SAS port.

  A and C SAS ports connect to the logical first shelf in a stack. B and D SAS ports connect to the logical last shelf in a stack.

- Port pairs use all SAS ports on each controller in your system.

  You increase system resiliency by incorporating all SAS ports (on an HBA in a physical PCI slot [slot 1-N] and on board the controller [slot 0]) into port pairs. Do not exclude any SAS ports.

- Port pairs are identified and organized as follows:

  a. List A ports and then C ports in sequence of slots (0,1, 2, 3, and so on).

     For example: 1a, 2a, 3a, 1c, 2c, 3c

  b. List B ports and then D ports in sequence of slots (0,1, 2, 3, and so on).

     For example: 1b, 2b, 3b, 1d, 2d, 3d

  c. Rewrite the D and B port list so that the first port in the list is moved to the end of the list.

For example: ~~1a~~, 2b, 3b, 1d, 2d, 3d, 1b

Offsetting the order of the slots by one balances port pairs across multiple slots (physical PCI slots and on board slots) when more than one slot of SAS ports is available; therefore, preventing a stack from being cabled to a single SAS HBA.

d. Pair the A and C ports (listed in step 1) to the D and B ports (listed in step 2) in the order that they are listed.

For example: 1a/2b, 2a/3b, 3a/1d,1c/2d, 2c/3d, 3c/1b.

> For an HA pair, the list of port pairs you identify for the first controller is also applicable to the second controller.

- When cabling your system, you can use port pairs in the order in which you identified them or you can skip port pairs:
  - Use port pairs in the order in which you identified (listed) them when all port pairs are needed to cable the stacks in your system.

    For example, if you identified six port pairs for your system and you have six stacks to cable as multipath, you cable the port pairs in the order in which you listed them:

    1a/2b, 2a/3b, 3a/1d,1c/2d, 2c/3d, 3c/1b

  - Skip port pairs (use every other port pair) when not all port pairs are needed to cable the stacks in your system.

    For example, if you identified six port pairs for your system and you have three stacks to cable as multipath, you cable every other port pair in your list:

    1a/2b, ~~2a/3b~~, 3a/1d, ~~1c/2d~~, 2c/3d, ~~3c/1b~~

> When you have more port pairs than you need to cable the stacks in your system, the best practice is to skip port pairs to optimize the SAS ports on your system. By optimizing SAS ports, you optimize your system's performance.

Controller-to-stack cabling worksheets are convenient tools for identifying and organizing port pairs so that you can cable the controller-to-stack connections for your HA pair or single-controller configuration.

Controller-to-stack cabling worksheet template for multipathed connectivity

Controller-to-stack cabling worksheet template for quad-pathed connectivity

AFF A200, AFF A220, FAS2600 series and FAS2700 controller 0b and 0a port connection rules to external disk shelves

The AFF A200, AFF A220, FAS2600 series and FAS2700 systems have a unique set of connection rules because each controller must maintain same domain connectivity between the internal storage (port 0b) and the stack. This means that when a controller is located in slot A of the chassis (controller 1) it is in domain A (IOM A) and therefore port 0b must connect to IOM A in the stack. When a controller is located in slot B of the chassis (controller 2) it is in domain B (IOM B) and therefore port 0b must connect to IOM B in the stack.

> If you do not connect the 0b port to the correct domain (cross-connect domains), you expose your system to resiliency issues that prevent you from performing nondisruptive procedures safely.

- Controller 0b port (internal storage port):
  - Controller 1 0b port always connects to IOM A (domain A).
  - Controller 2 0b port always connects to IOM B (domain B).
  - Port 0b is always the primary path.
  - Port 0b always connects to the logical last disk shelf in a stack.
  - Port 0b always connect to disk shelf IOM port 3.
- Controller 0a port (internal HBA port):
  - Controller 1 0a port always connects to IOM B (domain B).
  - Controller 2 0a port always connects to IOM A (domain A).
  - Port 0a is always the secondary path.
  - Port 0a always connects to the logical first disk shelf in a stack.
  - Port 0a always connect to disk shelf IOM port 1.

The following illustration highlights internal storage port (0b) domain connectivity for a AFF A200, AFF A220, FAS2600 series and FAS2700 multipath HA configuration:

Mini-SAS HD SAS optical cable rules

You can use mini-SAS HD SAS optical cables—multimode active optical cable (AOC) cables with mini-SAS HD-to-mini-SAS HD connectors and multimode (OM4) breakout cables with mini-SAS HD-to-LC connectors—to achieve long distance SAS connectivity for certain configurations that have disk shelves with IOM12 modules.

- Your platform and version of ONTAP must support the use of mini-SAS HD SAS optical cables: multimode active optical cable (AOC) cables with mini-SAS HD-to-mini-SAS HD connectors and multimode (OM4) breakout cables with mini-SAS HD-to-LC connectors.

  NetApp Hardware Universe

- SAS optical multimode AOC cables with mini-SAS HD-to-mini-SAS HD connectors can be used for controller-to-stack and shelf-to-shelf connections, and are available in lengths up to 50 meters.
- If you are using SAS optical multimode (OM4) breakout cables with mini-SAS HD-to-LC connectors (for patch panels), the following rules apply:
  - You can use these cables for controller-to-stack and shelf-to-shelf connections.

    If you use multimode breakout cables for shelf-to-shelf connections, you can only use them once within a stack of disk shelves. You must use multimode AOC cables to connect the remaining shelf-to-shelf connections.

    For quad-path HA and quad-path configurations, if you use multimode breakout cables for the shelf-to-shelf double-wide connections between two disk shelves, the best practice is to use identically paired breakout cables.

  - You must connect all eight (four pairs) of the LC breakout connectors to the patch panel.
  - You need to supply the patch panels and inter-panel cables.

    The inter-panel cables must be the same mode as the breakout cable: OM4 multimode.

  - Up to one pair of patch panels can be used in a path.
  - The point-to-point (mini-SAS HD-to-mini-SAS HD) path of any multimode cable cannot exceed 100 meters.

    The path includes the set of breakout cables, patch panels, and inter-panel cables.

  - The total end-to-end path (sum of point-to-point paths from the controller to the last shelf) cannot exceed 300 meters.

    The total path includes the set of breakout cables, patch panels, and inter-panel cables.

- The SAS cables can be SAS copper, SAS optical, or a mix.

  If you are using a mix of SAS copper cables and SAS optical cables, the following rules apply:

  - Shelf-to-shelf connections in a stack must be all SAS copper cables or all SAS optical cables.
  - If the shelf-to-shelf connections are SAS optical cables, the controller-to-stack connections to that stack must also be SAS optical cables.
  - If the shelf-to-shelf connections are SAS copper cables, the controller-to-stack connections to that stack can be SAS optical cables or SAS copper cables.

Controller-to-stack cabling worksheets and cabling examples for common multipath HA configurations - shelves with IOM12 modules

You can use the controller-to-stack cabling worksheets and cabling examples to cable your HA pair as a multipath HA configuration.

- If needed, you can refer to SAS cabling rules for information about supported configurations, the controller slot numbering convention, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including the use of port pairs).
- If needed, you can refer to How to read a worksheet to cable controller-to-stack connections for multipathed connectivity.
- Cabling examples show controller-to-stack cables as solid or dashed to distinguish controller A and C port connections from controller B and D port connections.

Controller-to-Stack Cable Type Key	
Cable Type	Description
	▪ Connects controller **A** and **C** ports to the logical **first** disk shelf in a stack ▪ The **primary** path from a controller to a stack
	▪ Connects controller **B** and **D** ports to the logical **last** disk shelf in a stack ▪ The **secondary** path from a controller to a stack

- Cables in the cabling examples and their corresponding port pairs in the worksheets are color-coded to distinguish connectivity to each stack in the HA pair.

Controller-to-Stack Cable Color Key			
Cable Color		Connects to...	From...
	Dark blue	Stack 1	Each controller by a unique port pair
	Orange	Stack 2	
	Green	Stack 3	
	Light blue	Stack 4	

- Worksheets and cabling examples show cabling port pairs in the order in which they are listed in the worksheet.

Controller-to-stack cabling worksheets and cabling examples for multipath HA configurations with quad-port SAS HBAs

You can use the completed controller-to-stack cabling worksheets and cabling examples to cable common multipath HA configurations that have quad-port SAS HBAs. These

controllers do not have onboard SAS ports.

Multipath HA with one quad-port SAS HBA and one single-shelf stack

The following worksheet and cabling example uses port pair 1a/1d:

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	1c				
	2	First	B	1						
B and D					~~1b~~	~~1d~~				
	1	Last	B	3	1d	1b				
	2	Last	A	3						

Multipath HA with one quad-port SAS HBA and two single-shelf stacks

The following worksheet and cabling example uses port pairs 1a/1d and 1c/1b:

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	1c				
	2	First	B	1						
B and D					~~1b~~	~~1d~~				
	1	Last	B	3	1d	1b				
	2	Last	A	3						

Multipath HA with two quad-port SAS HBAs and two multi-shelf stacks

Four port pairs are available for this configuration: 1a/2b, 2a/1d, 1c/2d, and 2c/1b. You can cable port pairs in the order in which they are identified (listed in the worksheet) or you can cable every other port pair (skip port pairs).

> When you have more port pairs than you need to cable the stacks in your system, the best practice is to skip port pairs to optimize the SAS ports on your system. By optimizing SAS ports, you optimize your system's performance.

The following worksheet and cabling example shows port pairs being used in the order in which they are listed in the worksheet: 1a/2b, 2a/1d, 1c/2d, and 2c/1b.

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	2a	1c	2c		
	2	First	B	1						
B and D					~~1b~~	~~2b~~	~~1d~~	~~2d~~		
	1	Last	B	3	2b	1d	2d	1b		
	2	Last	A	3						

The following worksheet and cabling example shows port pairs being skipped to use every other one in the list: 1a/2b and 1c/2d.

If a third stack is added later, you use the port pair that was skipped.

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	3 ~~2~~	2 ~~3~~	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	2a	1c	2c		
	2	First	B	1						
B and D					~~1b~~	~~2b~~	~~1d~~	~~2d~~		
	1	Last	B	3	2b	1d	2d	1b		
	2	Last	A	3						

Controller-to-stack cabling worksheets and cabling examples for multipath HA configurations with four onboard SAS ports

You can use the completed controller-to-stack cabling worksheets and cabling examples to cable common multipath HA configurations that have four onboard SAS ports.

Multipath HA with four onboard SAS ports and one single-shelf stack

The following worksheet and cabling example uses port pair 0a/0d:

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	0a	0c				
	2	First	B	1						
B and D					~~0b~~	~~0d~~				
	1	Last	B	3	0d	0b				
	2	Last	A	3						

Multipath HA with four onboard SAS ports and two single-shelf stacks

The following worksheet and cabling example uses port pairs 0a/0d and 0c/0b:

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	0a	0c				
	2	First	B	1						
B and D					~~0b~~	~~0d~~				
	1	Last	B	3	0d	0b				
	2	Last	A	3						

Multipath HA with four onboard SAS ports, a quad-port SAS HBA, and two multi-shelf stacks

Four port pairs are available for this configuration: 0a/1b, 1a/0d, 0c/1d, and 1c/0b. You can cable port pairs in the order in which they are identified (listed in the worksheet) or you can cable every other port pair (skip port pairs).

> When you have more port pairs than you need to cable the stacks in your system, the best practice is to skip port pairs to optimize the SAS ports on your system. By optimizing SAS ports, you optimize your system's performance.

The following worksheet and cabling example shows port pairs being used in the order in which they are listed in the worksheet: 0a/1b, 1a/0d, 0c/1d, and 1c/0b.

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	0a	1a	0c	1c		
	2	First	B	1						
B and D					~~0b~~	~~1b~~	~~0d~~	~~1d~~		
	1	Last	B	3	1b	0d	1d	0b		
	2	Last	A	3						

The following worksheet and cabling example shows port pairs being skipped to use every other one in the list: 0a/1b and 0c/1d.

> If a third stack is added later, you use the port pair that was skipped.

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	3 ~~2~~	2 ~~3~~	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	0a	1a	0c	1c		
	2	First	B	1						
B and D					~~0b~~	~~1b~~	~~0d~~	~~1d~~		
	1	Last	B	3	1b	0d	1d	0b		
	2	Last	A	3						

Controller-to-stack cabling worksheets and cabling examples for common AFF A200, AFF A220, FAS2600 series and FAS2700 configurations - shelves with IOM12 modules

You can use the completed controller-to-stack cabling worksheets and cabling examples to cable common AFF A200, AFF A220, FAS2600 series and FAS2700 configurations.

- If needed, you can refer to SAS cabling rules for information about supported configurations, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including AFF A200, AFF A220, FAS2600 series and FAS2700 port 0b same domain connectivity).
- Cabling examples show controller-to-stack cables as solid or dashed to distinguish controller 0b port connections from controller 0a port connections.

AFF A200, AFF A220, FAS2600, and FAS2700 Series Controller-to-Stack Cable Type Key	
Cable Type	Description
▬▬▬▬	▪ Connects controller **0b** port to the logical **last** disk shelf in the stack ▪ The **primary** path from a controller to the stack The internal storage connection
- - - -	▪ Connects controller **0a** port to the logical **first** disk shelf in the stack ▪ The **secondary** path from a controller to the stack The internal HBA connection

- Cabling examples show controller-to-stack connections and shelf-to-shelf connections in two different colors to distinguish connectivity through IOM A (domain A) and IOM B (domain B).

AFF A200, AFF A220, FAS2600, and FAS2700 Series Cable Color Key		
Cable Color		Connects...
	Light blue	IOM A (domain A)
	Purple	IOM B (domain B)

AFF A200, AFF A220, FAS2600 series and FAS2700 multipath HA configuration with one multi-shelf stack

The following worksheet and cabling example uses port pair 0a/0b:

Controller-to-Stack Cabling Worksheet (AFF A200, AFF A220, FAS2600, and FAS2700 Series)										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	B	1	0a					
	2	First	A	1						
B and D	1	Last	A	3	0b					
	2	Last	B	3						

AFF A200, AFF A220, FAS2600, and FAS2700 series multipath HA configuration

FAS2600 series multipath configuration with one multi-shelf stack

The following worksheets and cabling examples use port pair 0a/0b.

In this example, the controller is installed in slot A of the chassis. When a controller is located in slot A of the chassis, its internal storage port (0b) is in domain A (IOM A); therefore, port 0b must connect to domain A (IOM A) in the stack.

Controller-to-Stack Cabling Worksheet (FAS2600 series)										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	B	1	0a					
	~~2~~	~~First~~	~~A~~	~~1~~						
B and D	1	Last	A	3	0b					
	~~2~~	~~Last~~	~~B~~	~~3~~						

In this example, the controller is installed in slot B of the chassis. When a controller is located in slot B of the chassis, its internal storage port (0b) is in domain B (IOM B); therefore, port 0b must connect to domain B (IOM B) in the stack.

Controller-to-Stack Cabling Worksheet (FAS2600 series)										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port		Port pairs				
A and C	1	First	B	1	0a					
	~~2~~	~~First~~	~~A~~	~~1~~						
B and D	1	Last	A	3	0b					
	~~2~~	~~Last~~	~~B~~	~~3~~						

FAS2600 series multipath configuration

Controller-to-stack cabling worksheet and cabling example for a quad-path HA configuration with two quad-port SAS HBAs - shelves with IOM12 modules

You can use the completed controller-to-stack cabling worksheet and cabling example to cable a quad-path HA configuration that has two quad-port SAS HBAs.

- If needed, you can refer to SAS cabling rules for information about supported configurations, the controller slot numbering convention, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including the use of port pairs).
- If needed, you can refer to How to read a worksheet to cable controller-to-stack connections for quad-pathed connectivity.
- The cabling example shows controller-to-stack cables as solid or dashed to distinguish controller A and C port connections from controller B and D port connections.

Controller-to-Stack Cable Type Key	
Cable Type	Description
	▪ Connects controller **A** and **C** ports to the logical **first** disk shelf in a stack ▪ The **primary** path from a controller to a stack
	▪ Connects controller **B** and **D** ports to the logical **last** disk shelf in a stack ▪ The **secondary** path from a controller to a stack

- Cables in the cabling examples and their corresponding port pairs in the worksheets are color-coded to distinguish connectivity to each stack in the HA pair.

Controller-to-Stack Cable Color Key			
Cable Color		Connects to...	From...
	Dark blue	Stack 1	Each controller by a unique port pair
	Orange	Stack 2	

- The cabling example visually distinguishes the two sets of multipathed cabling needed to achieve quad-pathed connectivity for each controller to each stack in an HA pair or single-controller configuration.

  The first set of multipathed cabling is referred to as “multipathed”. The second set of multipathed cabling is referred to as “quad-pathed”. The second set of cabling is referred to as “quad-pathed” because completing this set of cabling gives you the quad-pathed connectivity.

Controller-to-Stack Quad-Pathed Connectivity Key			
Quad-pathed connectivity consists of two sets of cabling		Shown by color-coded ports on controllers and IOMs	Description
Set 1	Multipathed	No color	Ports (on controllers and IOMs) cabled with multipathed connectivity are shown without a color.
Set 2	Quad-pathed	The cable color associated with the applicable stack	Ports (on controllers and IOMs) cabled with quad-pathed connectivity are the same color as the cables connecting the stack, as shown in the “Controller-to-Stack Cable Color Key”.

- The worksheet example shows port pairs designated for multipathed cabling or quad-pathed cabling to the applicable stack.

  Each port pair designated for multipathed cabling is encircled by an oval that is the color associated with the stack it is cabled to. Each port pair designated for quad-pathed cabling is encircled by a rectangle that is the color associated with the stack it is cabled to.

Quad-path HA with two quad-port SAS HBAs and two multi-shelf stacks

The following worksheet and cabling example uses port pairs 1a/2b (multipathed) and 2a/1d (quad-pathed) for stack 1, and port pairs 1c/2d (multipathed) and 2c/1b (quad-pathed) for stack2.

Controller-to-Stack Cabling Worksheet for Quad-Pathed Connectivity									
Controller SAS ports	Controllers	Cable to disk shelf IOMs				Stacks			
		Shelf	IOM	Port		1		2	
				Multipathed	Quad-pathed	Port pairs			
A and C	1	First	A	1	2	1a	2a	1c	2c
	2	First	B	1	2				
B and D						~~1b~~	~~2b~~	~~1d~~	~~2d~~
	1	Last	B	3	4	2b	1d	2d	1b
	2	Last	A	3	4				

Controller-to-stack cabling worksheet template for multipathed connectivity - shelves with IOM12 modules

By completing the worksheet template, you can define the controller SAS port pairs you can use to cable controllers to stacks of disk shelves with IOM12 modules to achieve multipathed connectivity in an HA pair or single-controller configuration. You can also use the completed worksheet to walk yourself through cabling the multipathed connections for your configuration.

Before you begin

Your HA pair or single-controller configuration cannot be an AFF A200, AFF A220, FAS2600 series or FAS2700 system. If you have one of these configurations, use the following:

Controller-to-stack cabling worksheets and cabling examples for common AFF A200, AFF A220, FAS2600 series and FAS2700 configurations

About this task

- This procedure and worksheet template is applicable to cabling multipathed connectivity for a multipath HA or multipath configuration with one or more stacks.

  Examples of completed worksheets are provided for multipath HA and multipath configurations.

A configuration with two quad-port SAS HBAs and two stacks of disk shelves with IOM12 modules is used for the worksheet examples.

- The worksheet template allows for up to six stacks; you need to add more columns if needed.
- If needed, you can refer to the SAS cabling rules for information about supported configurations, the controller slot numbering convention, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including use of port pairs).
- If needed, after you complete the worksheet, you can refer to How to read a worksheet to cable controller-to-stack connections for multipathed connectivity

Controller-to-Stack Cabling Worksheet Multipathed Connectivity											
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks						
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1						
	2	First	B	1						
B and D										
	1	Last	B	3						
	2	Last	A	3						

Steps

1. In the boxes above the gray boxes, list all SAS A ports on your system, and then all SAS C ports on your system in sequence of slots (0,1, 2, 3, and so on).

   For example: 1a, 2a, 1c, 2c

2. In the gray boxes, list all SAS B ports on your system, and then all SAS D ports on your system in sequence of slots (0,1, 2, 3 and so on).

   For example: 1b, 2b, 1d, 2d

3. In the boxes below the gray boxes, rewrite the D and B port list so that the first port in the list is moved to the end of the list.

   For example: 2b, 1d, 2d, 1b

4. Circle (designate) a port pair for each stack.

   When all port pairs are being used to cable the stacks in your system, circle port pairs in the order in which they are defined (listed) in the worksheet.

   For example, in a multipath HA configuration with eight SAS ports and four stacks, port pair 1a/2b is cabled to stack 1, port pair 2a/1d is cabled to stack 2, port pair 1c/2d is cabled to stack3, and port pair 2c/1b is cabled to stack 4.

Controller-to-Stack Cabling Worksheet for Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	2a	1c	2c		
	2	First	B	1						
B and D					~~1b~~	~~2b~~	~~1d~~	~~2d~~		
	1	Last	B	3	2b	1d	2d	1b		
	2	Last	A	3						

When not all port pairs are needed to cable the stacks in your system, skip port pairs (use every other port pair).

For example, in a multipath HA configuration with eight SAS ports and two stacks, port pair 1a/2b is cabled to stack 1 and port pair 1c/2d is cabled to stack 2. If two additional stacks are hot-added later, port pair 2a/1d is cabled to stack 3 and port pair 2c/1b is cabled to stack 4.

> When you have more port pairs than you need to cable the stacks in your system, the best practice is to skip port pairs to optimize the SAS ports on your system. By optimizing SAS ports, you optimize your system's performance.

Controller-to-Stack Cabling Worksheet Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	3 ~~2~~	2 ~~3~~	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	2a	1c	2c		
	2	First	B	1						
B and D					~~1b~~	~~2b~~	~~1d~~	~~2d~~		
	1	Last	B	3	2b	1d	2d	1b		
	2	Last	A	3						

You can use your completed worksheet to cable your system.

5. If you have a single-controller (multipath) configuration, cross out the information for controller 2.

Controller-to-Stack Cabling Worksheet Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	2	3	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	2a	1c	2c		
	~~2~~	~~First~~	~~B~~	~~1~~						
B and D					~~1b~~	~~2b~~	~~1d~~	~~2d~~		
	1	Last	B	3	2b	1d	2d	1b		
	~~2~~	~~Last~~	~~A~~	~~3~~						

You can use your completed worksheet to cable your system.

Controller-to-stack cabling worksheet template for quad-pathed connectivity - shelves with IOM12 modules

By completing the worksheet template, you can define the controller SAS port pairs you can use to cable controllers to stacks of disk shelves with IOM12 modules to achieve quad-pathed connectivity in an HA pair or single-controller configuration. You can also use the completed worksheet to walk yourself through cabling the quad-pathed connections for your configuration.

About his task

- This procedure and worksheet template is applicable to cabling quad-pathed connectivity for a quad-path HA or quad-path configuration with one or more stacks.

  Examples of completed worksheets are provided for quad-path HA and quad-path configurations.

  A configuration with two quad-port SAS HBAs and two stacks of disk shelves with IOM12 modules is used for the worksheet examples.

- The worksheet template allows for up to two stacks; you need to add more columns if needed.
- Quad-pathed connectivity for controller-to-stack connections consists of two sets of multipathed cabling: the first set of cabling is referred to as “multipathed”; the second set of cabling is referred to as “quad-pathed”.

  The second set of cabling is referred to as “quad-pathed” because completing this set of cabling gives you the quad-pathed connectivity from a controller to a stack in an HA pair or single-controller configuration.

- Disk shelf IOM ports 1 and 3 are always used for multipathed cabling and IOM ports 2 and 4 are always used for quad-pathed cabling, as designated by the worksheet column headings.
- In the worksheet examples, port pairs are designated for multipathed cabling or quad-pathed cabling to the applicable stack.

  Each port pair designated for multipathed cabling is encircled by an oval that is the color associated with the stack it is cabled to. Each port pair designated for quad-pathed cabling is encircled by a rectangle that is the color associated with the stack it is cabled to. Stack 1 is associated with the color blue; stack 2 is associated with the color orange.

- If needed, you can refer to SAS cabling rules for information about the controller slot numbering convention, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including the use of port pairs).
- If needed, after you complete the worksheet, you can refer to How to read a worksheet to cable controller-to-stack connections for quad-pathed connectivity.

Controller-to-Stack Cabling Worksheet for Quad-Pathed Connectivity									
Controller SAS ports	Controllers	Cable to disk shelf IOMs				Stacks			
		Shelf	IOM	Port		1		2	
				Multipathed	Quad-pathed	Port pairs			
A and C	1	First	A	1	2				
	2	First	B	1	2				
B and D									
	1	Last	B	3	4				
	2	Last	A	3	4				

Steps

1. In the boxes above the gray boxes, list all SAS A ports on your system, and then all SAS C ports on your system in sequence of slots (0,1, 2, 3, and so on).

   For example: 1a, 2a, 1c, 2c

2. In the gray boxes, list all SAS B ports on your system, and then all SAS D ports on your system in sequence of slots (0,1, 2, 3 and so on).

   For example: 1b, 2b, 1d, 2d

3. In the boxes below the gray boxes, rewrite the D and B port list so that the first port in the list is moved to the end of the list.

   For example: 2b, 1d, 2d, 1b

4. Identify the two sets of port pairs to connect to stack 1 by drawing an oval around the first set of port pairs and a rectangle around the second set of port pairs.

   Both sets of cabling are needed to achieve quad-pathed connectivity from each controller to stack 1 in your HA pair or single-controller configuration.

   The following example uses port pair 1a/2b for the multipathed cabling and port pair 2a/1d for the quad-pathed cabling to stack 1.

Controller-to-Stack Cabling Worksheet for Quad-Pathed Connectivity									
Controller SAS ports	Controllers	Cable to disk shelf IOMs				Stacks			
		Shelf	IOM	Port		1		2	
				Multipathed	Quad-pathed	Port pairs			
A and C	1	First	A	1	2	1a	2a	1c	2c
	2	First	B	1	2				
B and D						~~1b~~	~~2b~~	~~1d~~	~~2d~~
	1	Last	B	3	4	2b	1d	2d	1b
	2	Last	A	3	4				

5. Identify the two sets of port pairs to connect to stack 2 by drawing an oval around the first set of port pairs and a rectangle around the second set of port pairs.

   Both sets of cabling are needed to achieve quad-pathed connectivity from each controller to stack 1 in your HA pair or single-controller configuration.

   The following example uses port pair 1c/2d for the multipathed cabling and port pair 2c/1b for the quad-pathed cabling to stack 2.

Controller-to-Stack Cabling Worksheet for Quad-Pathed Connectivity									
Controller SAS ports	Controllers	Cable to disk shelf IOMs				Stacks			
		Shelf	IOM	Port		1		2	
				Multipathed	Quad-pathed	Port pairs			
A and C	1	First	A	1	2	1a	2a	1c	2c
	2	First	B	1	2				
B and D						~~1b~~	~~2b~~	~~1d~~	~~2d~~
	1	Last	B	3	4	2b	1d	2d	1b
	2	Last	A	3	4				

6. If you have a quad-path (single-controller) configuration, cross out the information for controller 2; you only need controller 1 information to cable the controller-to-stack connections.

   The following example shows that the information for controller 2 is crossed out.

Controller-to-Stack Cabling Worksheet for Quad-Pathed Connectivity									
Controller SAS ports	Controllers	Cable to disk shelf IOMs				Stacks			
		Shelf	IOM	Port		1		2	
				Multipathed	Quad-pathed	Port pairs			
A and C	1	First	A	1	2	1a	2a	1c	2c
	~~2~~	~~First~~	~~B~~	~~1~~	~~2~~				
B and D						~~1b~~	~~2b~~	~~1d~~	~~2d~~
	1	Last	B	3	4	2b	1d	2d	1b
	~~2~~	~~Last~~	~~A~~	~~3~~	~~4~~				

How to read a worksheet to cable controller-to-stack connections for multipathed connectivity - shelves with IOM12 modules

You can use this example to guide you through how to read and apply a completed worksheet to cable controller-to-stack connections for disk shelves with IOM12 modules for multipathed connectivity.

Before you begin

Your HA pair or single-controller configuration cannot be an AFF A200, AFF A220, FAS2600 series or FAS2700 system. These systems use a unique worksheet:

Controller-to-stack cabling worksheets and cabling examples for common AFF A200, AFF A220, FAS2600 series and FAS2700 configurations

About this task

- This procedure references the following worksheet and cabling example to demonstrate how to read a worksheet to cable controller-to-stack connections.

  The configuration used in this example is a multipath HA configuration with two quad-port SAS HBAs (eight SAS ports) on each controller and two stacks of disk shelves with IOM12 modules. Port pairs are cabled by skipping every other port pair in the worksheet.

  > When you have more port pairs than you need to cable the stacks in your system, the best practice is to skip port pairs to optimize the SAS ports on your system. By optimizing SAS ports, you optimize your system's performance.

- If you have a single-controller configuration, skip substeps b and d for cabling to a second controller.
- If needed, you can refer to SAS cabling rules for information about the controller slot numbering convention, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including the use of port pairs).

The port pairs are cabled using every other port pair in the worksheet: 1a/2b and 1c/2d.

Controller-to-Stack Cabling Worksheet Multipathed Connectivity										
Controller SAS ports	Controllers	Cable to disk shelf IOMs			Stacks					
					1	3 ~~2~~	2 ~~3~~	4	5	6
		Shelf	IOM	Port	Port pairs					
A and C	1	First	A	1	1a	2a	1c	2c		
	2	First	B	1						
B and D					~~1b~~	~~2b~~	~~1d~~	~~2d~~		
	1	Last	B	3	2b	1d	2d	1b		
	2	Last	A	3						

Multipath HA configuration

Steps

1. Cable port pair 1a/2b on each controller to stack 1:
   a. Cable controller 1 port 1a to stack 1, first shelf IOM A port 1.
   b. Cable controller 2 port 1a to stack 1, first shelf IOM B port 1.

c. Cable controller 1 port 2b to stack 1, last shelf IOM B port 3.

d. Cable controller 2 port 2b to stack 1, last shelf IOM A port 3.

2. Cable port pair 1c/2d on each controller to stack 2:

   a. Cable controller 1 port 1c to stack 2, first shelf IOM A port 1.

   b. Cable controller 2 port 1c to stack 2, first shelf IOM B port 1.

   c. Cable controller 1 port 2d to stack 2, last shelf IOM B port 3.

   d. Cable controller 2 port 2d to stack 2, last shelf IOM A port 3.

How to read a worksheet to cable controller-to-stack connections for quad-pathed connectivity - shelves with IOM12 modules

You can use this example to guide you through how to read and apply a completed worksheet to cable stacks of disk shelves with IOM12 modules for quad-pathed connectivity.

About this task

- This procedure references the following worksheet and cabling example to demonstrate how to read a worksheet to cable controller-to-stack connections.

  The configuration used in this example is a quad-path HA configuration with two quad-port SAS HBAs on each controller and two stacks of disk shelves with IOM12 modules.

- If you have a single-controller configuration, skip substeps b and d for cabling to a second controller.
- If needed, you can refer to SAS cabling rules for information about the controller slot numbering convention, shelf-to-shelf connectivity, and controller-to-shelf connectivity (including the use of port pairs).

Controller-to-Stack Cabling Worksheet for Quad-Pathed Connectivity									
Controller SAS ports	Controllers	Cable to disk shelf IOMs				Stacks			
		Shelf	IOM	Port		1		2	
				Multipathed	Quad-pathed	Port pairs			
A and C	1	First	A	1	2	1a	2a	1c	2c
	2	First	B	1	2				
B and D						~~1b~~	~~2b~~	~~1d~~	~~2d~~
	1	Last	B	3	4	2b	1d	2d	1b
	2	Last	A	3	4				

Steps

1. Cable port pair 1a/2b on each controller to stack 1:

   This is the multipathed cabling for stack 1.

   a. Cable controller 1 port 1a to stack 1, first shelf IOM A port 1.
   b. Cable controller 2 port 1a to stack 1, first shelf IOM B port 1.
   c. Cable controller 1 port 2b to stack 1, last shelf IOM B port 3.
   d. Cable controller 2 port 2b to stack 1, last shelf IOM A port 3.

2. Cable port pair 2a/1d on each controller to stack 1:

   This is the quad-pathed cabling for stack 1. Once completed, stack 1 has quad-pathed connectivity to each controller.

   a. Cable controller 1 port 2a to stack 1, first shelf IOM A port 2.
   b. Cable controller 2 port 2a to stack 1, first shelf IOM B port 2.
   c. Cable controller 1 port 1d to stack 1, last shelf IOM B port 4.
   d. Cable controller 2 port 1d to stack 1, last shelf IOM A port 4.

3. Cable port pair 1c/2d on each controller to stack 2:

   This is the multipathed cabling for stack 2.

   a. Cable controller 1 port 1c to stack 2, first shelf IOM A port 1.
   b. Cable controller 2 port 1c to stack 2, first shelf IOM B port 1.
   c. Cable controller 1 port 2d to stack 2, last shelf IOM B port 3.
   d. Cable controller 2 port 2d to stack 2, last shelf IOM A port 3.

4. Cable port pair 2c/1b on each controller to stack 2:

   This is the quad-pathed cabling for stack 2. Once completed, stack 2 has quad-pathed connectivity to each controller.

   a. Cable controller 1 port 2c to stack 2, first shelf IOM A port 2.
   b. Cable controller 2 port 2c to stack 2, first shelf IOM B port 2.
   c. Cable controller 1 port 1b to stack 2, last shelf IOM B port 4.
   d. Cable controller 2 port 1b to stack 2, last shelf IOM A port 4.

Maintain

Hot-swap a disk drive in a DS224C or DS212C disk shelf - shelves with IOM12 modules

You can hot-swap a failed disk drive in a DS224C or DS212C disk shelf.

Before you begin

- The disk drive that you are installing must be supported by the DS224C or DS212C disk shelf.

  NetApp Hardware Universe

- All other components in the system must be functioning properly; if not, contact technical support.
- The disk drive you are removing must be failed.

  You can verify the disk drive is failed by running the `storage disk show -broken` command. The failed disk drive appears in the list of failed disk drives. If it does not, you should wait, and run the command again.

  > Depending on the disk drive type and capacity, it can take up to several hours for the disk drive to appear in the list of failed disk drives.

- If you are replacing a self-encrypting disk (SED), you must follow the instructions for Replacing an SED in the ONTAP documentation for your version of ONTAP.

  Instructions in the ONTAP documentation describe additional steps you must perform before and after replacing an SED.

  NetApp encryption overview with the CLI

About this task

- You should take steps to avoid electrostatic discharge (ESD):

- Keep the disk drive in the ESD bag until you are ready to install it.
- Open the ESD bag by hand or cut the top off with a pair of scissors.

  Do not insert a metal tool or knife into the ESD bag.

- Always wear an ESD wrist strap grounded to an unpainted surface on your storage enclosure chassis.

  If a wrist strap is unavailable, touch an unpainted surface on your storage enclosure chassis before handling the disk drive.

- You should take steps to handle disk drives carefully:
  - Always use two hands when removing, installing, or carrying a disk drive to support its weight.

    Do not place hands on the disk drive boards exposed on the underside of the disk drive carrier.

  - You should place disk drives on cushioned surfaces, and never stack disk drives on top of each other.
  - You should be careful not to bump disk drives against other surfaces.
- Disk drives should be kept away from magnetic devices.

  Magnetic fields can destroy all data on the disk drive and cause irreparable damage to the disk drive circuitry.

- The best practice is to have the current version of the Disk Qualification Package (DQP) installed before hot-swapping a disk drive.

  Having the current version of the DQP installed allows your system to recognize and utilize newly qualified disk drives; therefore, avoiding system event messages about having non-current disk drive information. You also avoid the possible prevention of disk partitioning because disk drives are not recognized. The DQP also notifies you of non-current disk drive firmware.

  NetApp Downloads: Disk Qualification Package

- The best practice is to have the current versions of disk shelf (IOM) firmware and disk drive firmware on your system before adding new disk shelves, shelf FRU components, or SAS cables.

  Current versions of firmware can be found on the NetApp Support Site.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

- Disk drive firmware is automatically updated (nondisruptively) on new disk drives with non current firmware versions.

  Disk drive firmware checks occur every two minutes.

- If needed, you can turn on the disk shelf's location (blue) LEDs to aid in physically locating the affected disk shelf: `storage shelf location-led modify -shelf-name` *`shelf_name`* `-led-status on`

  A disk shelf has three location LEDs: one on the operator display panel and one on each IOM12 module.

Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

- If needed, you can refer to the Monitoring disk shelf LEDs section for information about the meaning and location of disk shelf LEDs on the operator display panel and FRU components.

Steps

1. If you want to manually assign disk ownership for the replacement disk drive, you need to disable automatic drive assignment if it is enabled; otherwise, go to the next step.

   > You need to manually assign disk ownership if disk drives in the stack are owned by both controllers in an HA pair.

   > You manually assign disk ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify if automatic drive assignment is enabled:`storage disk option show`

      If you have an HA pair, you can enter the command at the console of either controller.

      If automatic drive assignment is enabled, the output shows “on” (for each controller) in the “Auto Assign” column.

   b. If automatic drive assignment is enabled, you need to disable it:`storage disk option modify -node` *`node_name`* `-autoassign off`

      You need to disable automatic drive assignment on both controllers in an HA pair.

2. Properly ground yourself.
3. Unpack the new disk drive, and set it on a level surface near the disk shelf.

   Save all packaging materials for use when returning the failed disk drive.

   > NetApp requires that all returned disk drives be in a ESD-rated bag.

4. Physically identify the failed disk drive from the system console warning message and the illuminated attention (amber) LED on the disk drive.

   > The activity (green) LED on a failed disk drive can be illuminated (solid), which indicates the disk drive has power, but should not be blinking, which indicates I/O activity. A failed disk drive has no I/O activity.

5. Press the release button on the disk drive face, and then pull the cam handle to its fully open position to release the disk drive from the mid plane.

   When you press the release button, the cam handle on the disk drive springs open partially.

   > Disk drives in a DS212C disk shelf are arranged horizontally with the release button located on the left of the disk drive face. Disk drives in a DS224C disk shelf are arranged vertically with the release button located at the top of the disk drive face.

   The following shows disk drives in a DS212C disk shelf:

The following shows disk drives in a DS224C disk shelf:

6. Slide out the disk drive slightly to allow the disk to safely spin down, and then remove the disk drive from the disk shelf.

   An HDD can take up to one minute to safely spin down.

   When handling a disk drive, always use two hands to support its weight.

7. Using two hands, with the cam handle in the open position, insert the replacement disk drive into the disk shelf, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   Do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

8. Close the cam handle so that the disk drive is fully seated into the mid plane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive.

9. If you are replacing another disk drive, repeat Steps 3 through 8.

10. Verify the disk drive's activity (green) LED is illuminated.

    When the disk drive's activity LED is solid green, it means the disk drive has power. When the disk drive's activity LED is blinking, it means the disk drive has power and I/O is in progress. If the disk drive firmware is automatically updating, the LED will be blinking.

11. If you disabled automatic drive assignment in Step 1, manually assign disk ownership, and then reenable automatic drive assignment if needed:

    a. Display all unowned disks:`storage disk show -container-type unassigned`

    b. Assign each disk:`storage disk assign -disk disk_name -owner owner_name`

       You can use the wildcard character to assign more than one disk at once.

    c. Reenable automatic drive assignment if needed:`storage disk option modify -node node_name -autoassign on`

       You need to reenable automatic drive assignment on both controllers in an HA pair.

12. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a disk drive in a DS460C disk shelf - shelves with IOM12 modules

You can hot-swap a failed disk drive in a DS460C disk shelf.

Before you begin

- The replacement disk drive must be supported by the DS460C disk shelf.

  NetApp Hardware Universe

- All other components in the system must be functioning properly; if not, contact technical support.
- The disk drive you are removing must be failed.

  You can verify the disk drive is failed by running the `storage disk show -broken` command. The failed disk drive appears in the list of failed disk drives. If it does not, you should wait, and run the command again.

  > Depending on the disk drive type and capacity, it can take up to several hours for the disk drive to appear in the list of failed disk drives.

- If you are replacing a self-encrypting disk (SED), you must follow the instructions for Replacing an SED in the ONTAP documentation for your version of ONTAP.

  Instructions in the ONTAP documentation describe additional steps you must perform before and after replacing an SED.

  NetApp encryption overview with the CLI

About this task

- You should take steps to avoid electrostatic discharge (ESD):
  - Keep the disk drive in the ESD bag until you are ready to install it.
  - Open the ESD bag by hand or cut the top off with a pair of scissors.

    Do not insert a metal tool or knife into the ESD bag.

  - Always wear an ESD wrist strap grounded to an unpainted surface on your storage enclosure chassis.

    If a wrist strap is unavailable, touch an unpainted surface on your storage enclosure chassis before handling the disk drive.

- You should take steps to handle disk drives carefully:
  - Always use two hands when removing, installing, or carrying a disk drive to support its weight.

    Do not place hands on the disk drive boards exposed on the underside of the disk drive carrier.

  - You should place disk drives on cushioned surfaces, and never stack disk drives on top of each other.
  - You should be careful not to bump disk drives against other surfaces.
- Disk drives should be kept away from magnetic devices.

  Magnetic fields can destroy all data on the disk drive and cause irreparable damage to the disk drive circuitry.

- The best practice is to have the current version of the Disk Qualification Package (DQP) installed before hot-swapping a disk drive.

  Having the current version of the DQP installed allows your system to recognize and utilize newly qualified disk drives; therefore, avoiding system event messages about having non-current disk drive information. You also avoid the possible prevention of disk partitioning because disk drives are not recognized. The DQP also notifies you of non-current disk drive firmware.

  NetApp Downloads: Disk Qualification Package

- The best practice is to have the current versions of disk shelf (IOM) firmware and disk drive firmware on your system before adding new disk shelves, shelf FRU components, or SAS cables.

  Current versions of firmware can be found on the NetApp Support Site.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

- Disk drive firmware is automatically updated (nondisruptively) on new disk drives with non current firmware versions.

  Disk drive firmware checks occur every two minutes.

- If needed, you can turn on the disk shelf's location (blue) LEDs to aid in physically locating the affected disk shelf: `storage shelf location-led modify -shelf-name` *`shelf_name`* `-led-status on`

A disk shelf has three location LEDs: one on the operator display panel and one on each IOM12 module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

- If needed, you can refer to the Monitoring disk shelf LEDs section for information about the meaning and location of disk shelf LEDs on the operator display panel and FRU components.
- The DS460C drive shelf consist of five drive drawers (drive drawer 1 at the top through drive drawer 5 at the bottom) that each contain 12 drive slots.

- The following illustration shows how the drives are numbered from 0 to 11 in each drive drawer within the shelf.

Steps

1. If you want to manually assign disk ownership for the replacement disk drive, you need to disable automatic drive assignment if it is enabled; otherwise, go to the next step.

> You need to manually assign disk ownership if disk drives in the stack are owned by both controllers in an HA pair.

> You manually assign disk ownership and then reenable automatic drive assignment later in this procedure.

a. Verify if automatic drive assignment is enabled:`storage disk option show`

   If you have an HA pair, you can enter the command at the console of either controller.

   If automatic drive assignment is enabled, the output shows “on” (for each controller) in the “Auto Assign” column.

b. If automatic drive assignment is enabled, you need to disable it:`storage disk option modify -node node_name -autoassign off`

   You need to disable automatic drive assignment on both controllers in an HA pair.

2. Properly ground yourself.
3. Unpack the new disk drive, and set it on a level surface near the disk shelf.

   Save all packaging materials for use when returning the failed disk drive.

   > NetApp requires that all returned disk drives be in a ESD-rated bag.

4. Identify the failed disk drive from the system console warning message and the illuminated amber attention LED on the drive drawer.

   The 2.5-inch and 3.5-inch SAS drive carriers do not contain LEDs. Instead, you must look at the Attention LEDs on the drive drawers to determine which drive has failed.

   The drive drawer’s Attention LED (amber) blinks so you can open the correct drive drawer to identify which drive to replace.

   The drive drawer’s Attention LED is on the front-left side in front of each drive, with a warning symbol on the drive handle just behind the LED.

5. Open the drawer containing the failed drive:
   a. Unlatch the drive drawer by pulling on both levers.
   b. Using the extended levers, carefully pull the drive drawer out until it stops.
   c. Look at the top of the drive drawer to find the Attention LED that resides on the drawer in front of each drive.
6. Remove the failed drive from the open drawer:
   a. Gently pull back the orange release latch that is in front of the drive you want to remove.

1	Orange release latch

b. Open the cam handle, and lift out the drive slightly.
c. Wait 30 seconds.
d. Use the cam handle to lift the drive from the shelf.

e. Place the drive on an antistatic, cushioned surface away from magnetic fields.

7. Insert the replacement drive in the drawer:
   a. Raise the cam handle on the new drive to vertical.
   b. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.

❶	Raised button on the right side of the drive carrier

c. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.

d. Carefully push the drive drawer back into the enclosure.

Possible loss of data access: Never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

e. Close the drive drawer by pushing both levers towards the center.

   The green Activity LED for the replaced drive on the front of the drive drawer comes on when the drive is inserted correctly.

8. If you are replacing another disk drive, repeat Steps 4 through 7.
9. Check the Activity LED and the Attention LED on the drive you replaced.

LED status	Description
The Activity LED is on or blinking, and the Attention LED is off	The new drive is working correctly.
The Activity LED is off	The drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
The Attention LED is on	The new drive might be defective. Replace it with another new drive. When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.

10. If you disabled disk ownership automatic assignment in Step 1, manually assign disk ownership, and then reenable disk ownership automatic assignment if needed:
    a. Display all unowned disks:`storage disk show -container-type unassigned`
    b. Assign each disk:`storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`*

       You can use the wildcard character to assign more than one disk at once.

    c. Reenable disk ownership automatic assignment if needed:`storage disk option modify -node` *`node_name`* `-autoassign on`

       You need to reenable disk ownership automatic assignment on both controllers in an HA pair.

11. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Replace a drive drawer in a DS460C disk shelf - shelves with IOM12 modules

You must stop all host I/O activity and power off the shelf before replacing the drive drawer.

Each of these 60-drive shelves has five drive drawers.

And each of the five drawers can hold up to 12 drives.

Before you begin

You need these items for this procedure:

- Antistatic protection

> **Possible hardware damage:** To prevent electrostatic discharge damage to the drive shelf, use proper antistatic protection when handling drive shelf components.

- Replacement drive drawer
- Replacement left and right cable chains
- Flashlight
- Permanent marker

Remove the cable chains

Left and right cable chains for each drive drawer in the DS460C drive shelf allow the drawers to slide in and out. Before you can remove a drive drawer, you must remove both cable chains.

Before you begin

- You have stopped host I/O activity and powered off the shelf.
- You have obtained the following items:
  - Antistatic protection

    Possible hardware damage: To prevent electrostatic discharge damage to the shelf, use proper antistatic protection when handling shelf components.

  - Flashlight

About this task

Each drive drawer has left and right cable chains. The metal ends on the cable chains slide into corresponding vertical and horizontal brackets inside the enclosure, as follows:

- The left and right vertical brackets connect the cable chain to the enclosure's midplane.
- The left and right horizontal brackets connect the cable chain to the individual drawer.

Steps

1. Put on antistatic protection.
2. From the rear of the drive shelf, remove the right fan module, as follows:
   a. Press the orange tab to release the fan module handle.

      The figure shows the handle for the fan module extended and released from the orange tab on the left.

1	Fan module handle

b. Using the handle, pull the fan module out of the drive shelf, and set it aside.

3. Manually determine which of the five cable chains to disconnect.

   The figure shows the right side of the drive shelf with the fan module removed. With the fan module removed, you can see the five cable chains and the vertical and horizontal connectors for each drawer. The callouts for drive drawer 1 are provided.

2
1
3

1	Cable chain
2	Vertical connector (connected to the midplane)
3	Horizontal connector (connected to the drive drawer)

The top cable chain is attached to drive drawer 1. The bottom cable chain is attached to drive drawer 5.

4. Use your finger to move the cable chain on the right side to the left.
5. Follow these steps to disconnect any of the right cable chains from its corresponding vertical bracket.
   a. Using a flashlight, locate the orange ring on the end of the cable chain that is connected to the vertical bracket in the enclosure.

1	Orange ring on the vertical bracket

b. Disconnect the vertical connector (connected to the midplane) by gently pressing on the center of the

orange ring and pulling the left side of the cable out of the enclosure.

c. To unplug the cable chain, carefully pull your finger toward you approximately 1 inch (2.5 cm), but leave the cable chain connector within the vertical bracket.

6. Follow these steps to disconnect the other end of the cable chain:

   a. Using a flashlight, locate the orange ring on the end of the cable chain that is attached to the horizontal bracket in the enclosure.

      The figure shows the horizontal connector on the right and the cable chain disconnected and partially pulled out on the left side.

1	Orange ring on horizontal bracket
2	Cable chain

b. Gently insert your finger into the orange ring.

   The figure shows the orange ring on the horizontal bracket being pushed down so that the rest of the cable chain can be pulled out of the enclosure.

c. Pull your finger toward you to unplug the cable chain.

7. Carefully pull the entire cable chain out of the drive shelf.
8. From the back of the drive shelf, remove the left fan module.
9. Follow these steps to disconnect the left cable chain from its vertical bracket:
   a. Using a flashlight, locate the orange ring on the end of the cable chain attached to the vertical bracket.
   b. Insert your finger into the orange ring.
   c. To unplug the cable chain, pull your finger toward you approximately 1 inch (2.5 cm), but leave the cable chain connector within the vertical bracket.
10. Disconnect the left cable chain from the horizontal bracket, and pull the entire cable chain out of the drive shelf.

Remove a drive drawer

After removing the right and left cable chains, you can remove the drive drawer from the drive shelf. Removing a drive drawer entails sliding the drawer part of the way out, recording the locations of the drives, removing the drives, and removing the drive drawer.

Before you begin

- You have removed the right and left cable chains for the drive drawer.
- You have replaced the right and left fan modules.
- You have obtained a permanent marker to note the exact location of each drive as you remove the drive from the drawer.

Steps

1. Remove the bezel from the front of the drive shelf.
2. Unlatch the drive drawer by pulling out on both levers.
3. Using the extended levers, carefully pull the drive drawer out until it stops. Do not completely remove the drive drawer from the drive shelf.
4. If logical unit numbers (LUNs) have already been created and assigned, use a permanent marker to note the exact location of each drive. For example, using the following drawing as a reference, write the appropriate slot number on the top of each drive.

Possible loss of data access: Make sure to record the exact location of each drive before removing it.

5. Remove the drives from the drive drawer:
   a. Gently pull back the orange release latch that is visible on the center front of each drive. The following image shows the orange release latch for each of the drives.

b. Raise the drive handle to vertical.

c. Use the handle to lift the drive from the drive drawer.

d. Place the drive on a flat, static-free surface and away from magnetic devices.

> **Possible loss of data access:** Magnetic fields can destroy all data on the drive and cause irreparable damage to the drive circuitry. To avoid loss of data access and damage to the drives, always keep drives away from magnetic devices.

6. Follow these steps to remove the drive drawer:

   a. Locate the plastic release lever on each side of the drive drawer.

1	Drive drawer release lever

   b. Open both release levers by pulling the latches toward you.

c. While holding both release levers, pull the drive drawer toward you.

d. Remove the drive drawer from the drive shelf.

Install a drive drawer

Installing a drive drawer into a drive shelf entails sliding the drawer into the empty slot, installing the drives, and replacing the front bezel.

Before you begin

- You know where to install each drive.
- You have obtained the following items:
  - Replacement drive drawer
  - Flashlight

Steps

1. From the front of the drive shelf, shine a flashlight into the empty drawer slot, and locate the lock-out tumbler for that slot.

   The lock-out tumbler assembly is a safety feature that prevents you from being able to open more than one drive drawer at one time.

1	Lock-out tumbler
2	Drawer guide

2. Position the replacement drive drawer in front of the empty slot and slightly to the right of center.

Positioning the drawer slightly to the right of center helps to ensure that the lock-out tumbler and the drawer guide are correctly engaged.

3. Slide the drive drawer into the slot, and ensure that the drawer guide slides under the lock-out tumbler.

> **Risk of equipment damage:** Damage occurs if the drawer guide does not slide under the lock-out tumbler.

4. Carefully push the drive drawer all the way in until the latch fully engages.

> **Risk of equipment damage:** Stop pushing the drive drawer if you feel excessive resistance or binding. Use the release levers at the front of the drawer to slide the drawer back out. Then, reinsert the drawer into the slot, and ensure that it slides in and out freely.

5. Follow these steps to reinstall the drives in the drive drawer:
   a. Unlatch the drive drawer by pulling out on both levers at the front of the drawer.
   b. Using the extended levers, carefully pull the drive drawer out until it stops. Do not completely remove the drive drawer from the drive shelf.
   c. Determine which drive to install in each slot by using the notes you made when removing the drives.

> **Possible loss of data access:** You must install each drive in its original location in the drive drawer.

   d. Raise the handle on the drive to vertical.
   e. Align the two raised buttons on each side of the drive with the notches on the drawer.

      The figure shows the right side view of a drive, showing the location of the raised buttons.

❶	Raised button on the right side of the drive.

f. Lower the drive straight down, and then rotate the drive handle down until the drive snaps into place.

g. Repeat these substeps to reinstall all of the drives.

6. Slide the drawer back into the drive shelf by pushing it from the center and closing both levers.

> **Risk of equipment malfunction:** Make sure to completely close the drive drawer by pushing both levers. You must completely close the drive drawer to allow proper airflow and prevent overheating.

7. Attach the bezel to the front of the drive shelf.

Attach the cable chains

The final step in installing a drive drawer is attaching the left and right cable chains to the drive shelf. When attaching a cable chain, reverse the order you used when disconnecting the cable chain. You must insert the chain's horizontal connector into the horizontal bracket in the enclosure before inserting the chain's vertical connector into the vertical bracket in the enclosure.

Before you begin

- You have replaced the drive drawer and all of the drives.
- You have two replacement cable chains, marked as LEFT and RIGHT (on the horizontal connector next to the drive drawer).

Callout	Cable chain	Connector	Connects to
1	Left	Vertical	Midplane
2	Left	Horizontal	Drive drawer

Callout	Cable chain	Connector	Connects to
1	Right	Horizontal	Drive drawer
2	Right	Vertical	Midplane

Steps

1. Follow these steps to attach the left cable chain:
   a. Locate the horizontal and vertical connectors on the left cable chain and the corresponding horizontal and vertical brackets inside the enclosure.
   b. Align both cable chain connectors with their corresponding brackets.
   c. Slide the cable chain's horizontal connector under the guide rail on the horizontal bracket, and push it in as far as it can go.

      The figure shows the guide rail on the left side for the second drive drawer in the enclosure.

1	Guide rail

> **Risk of equipment malfunction:** Make sure to slide the connector underneath the guide rail on the bracket. If the connector rests on the top of the guide rail, problems might occur when the system runs.

d. Slide the vertical connector on the left cable chain into the vertical bracket.

e. After you have reconnected both ends of the cable chain, carefully pull on the cable chain to verify that both connectors are latched.

> **Risk of equipment malfunction:** If the connectors are not latched, the cable chain might come loose during drawer operation.

2. Reinstall the left fan module.
3. Follow these steps to reattach the right cable chain:
   a. Locate the horizontal and vertical connectors on the cable chain and their corresponding horizontal and vertical brackets inside the enclosure.
   b. Align both cable chain connectors with their corresponding brackets.
   c. Slide the cable chain's horizontal connector under the guide rail on the horizontal bracket and push it in as far as it will go.

> **Risk of equipment malfunction:** Make sure to slide the connector underneath the guide rail on the bracket. If the connector rests on the top of the guide rail, problems might occur when the system runs.

   d. Slide the vertical connector on the right cable chain into the vertical bracket.
   e. After you reconnect both ends of the cable chain, carefully pull on the cable chain to verify that both connectors are latched.

> **Risk of equipment malfunction:** If the connectors are not latched, the cable chain might come loose during drawer operation.

4. Reinstall the right fan module.
5. Reapply power:
   a. Turn on both power switches on the drive shelf.
   b. Confirm that both fans come on and that the amber LED on the back of the fans is off.

Replace a fan module in a DS460C disk shelf - shelves with IOM12 modules

Each DS460C drive shelf includes two fan modules. If a fan module fails, you must replace it as soon as possible to ensure that the shelf has adequate cooling. When you remove the failed fan module, you do not have to turn off power to your disk shelf.

About this task

You must ensure that you remove and replace the fan module within 30 minutes to prevent the system from overheating.

Steps

1. Put on antistatic protection.

2. Unpack the new fan module, and place it on a level surface near the shelf.

   Save all packing material for use when returning the failed fan.

3. From the back of the disk shelf, look at the Attention LEDs to locate the fan module you need to remove.

   You must replace the fan module that has its Attention LED on.

Item	LED name	State	Description
1	Attention	Solid amber	The fan has a fault

4. Press the orange tab to release the fan module handle.

1	Tab that you press to release the fan module handle

5. Use the fan module handle to pull the fan module out of the shelf.

1	Handle to pull the fan module out

6. Slide the replacement fan module all the way into the shelf, moving the fan module handle to the side until it latches with the orange tab.
7. Check the amber Attention LED on the new fan module.

> After you replace the fan module, the Attention LED stays on (solid amber) while the firmware checks that the fan module was installed correctly. The LED goes off after this process is complete.

8. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

   Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number.

Hot-remove a shelf - shelves with IOM12 modules

You can hot-remove a disk shelf with IOM12 modules—nondisruptively remove a disk shelf from a system that is powered on and serving data (I/O is in progress)--when you need to move or replace the disk shelf. You can hot-remove one or more disk shelves from anywhere within a stack of disk shelves or remove a stack of disk shelves.

Before you begin

- Your system must be a multipath HA, multipath, quad-path HA, or quad-path configuration.

  For AFF A200, AFF A220, FAS2600 series and FAS2700 systems, the external storage must be cabled as multipath HA or multipath.

  > For a FAS2600 series single-controller system that has the external storage cabled with multipath connectivity, the system is a mixed-path configuration because the internal storage uses single-path connectivity.

- Your system cannot have any SAS cabling error messages.

  You can download and run Active IQ Config Advisor to view any SAS cabling error messages and the corrective actions you should take.

  NetApp Downloads: Config Advisor

- HA pair configurations cannot be in a takeover state.
- You must have removed all aggregates from the disk drives—the disk drives must be spares-- in the disk shelves you are removing.

  > If you attempt this procedure with aggregates on the disk shelf you are removing, you could fail the system with a multidisk panic.

  You can use the `storage aggregate offline -aggregate` *`aggregate_name`* command and then the `storage aggregate delete -aggregate` *`aggregate_name`* command.

- If you are removing one or more disk shelves from within a stack, you must have factored the distance to bypass the disk shelves you are removing; therefore, if the current cables are not long enough, you need to have longer cables available.

About this task

- **Best practice:** The best practice is to remove disk drive ownership after you remove the aggregates from the disk drives in the disk shelves you are removing.

  Removing ownership information from a spare disk drive allows the disk drive to be properly integrated into another node (as needed).

  > The procedure for removing ownership from disk drives requires you to disable disk ownership automatic assignment. You reenable disk ownership automatic assignment at the end of this procedure.
  >
  > Disks and aggregates overview

- For a clustered ONTAP system that is greater than two-nodes, best practice is to have reassigned epsilon to an HA pair other than the one that is undergoing planned maintenance.

  Reassigning epsilon minimizes the risk of unforeseen errors impacting all nodes in a clustered ONTAP system. You can use the following steps to determine the node holding epsilon and reassign epsilon if needed:

  1. Set privilege level to advanced: `set -privilege advanced`

2. Determine which node holds epsilon: `cluster show`

   The node that holds epsilon shows `true` in the `Epsilon` column. (The nodes that do not hold epsilon show `false`.)

3. If the node in the HA pair that is undergoing maintenance shows `true` (holds epsilon), then remove epsilon from the node: `cluster modify -node node_name -epsilon false`
4. Assign epsilon to a node in another HA pair: `cluster modify -node node_name -epsilon true`
5. Return to the admin privilege level: `set -privilege admin`

- If you are hot-removing a disk shelf from a stack (but keeping the stack), you recable and verify one path at a time (path A then path B) to bypass the disk shelf you are removing so that you always maintain single-path connectivity from the controllers to the stack.

> If you do not maintain single-path connectivity from the controllers to the stack when recabling the stack to bypass the disk shelf you are removing, you could fail the system with a multidisk panic.

Steps

1. Verify that your system configuration is `Multi-Path HA`, `Multi-Path`, `Quad-path HA`, or `Quad-path`: `sysconfig`

   You run this command from the nodeshell of either controller. It might take up to a minute for the system to complete discovery.

   The configuration is listed in the `System Storage Configuration` field.

   > For a FAS2600 series single-controller system that has the external storage cabled with multipath connectivity, the output is displayed as `mixed-path` because the internal storage uses single-path connectivity.

2. Verify that the disk drives in the disk shelves you are removing have no aggregates (are spares) and ownership is removed:

   a. Enter the following command from the clustershell of either controller: `storage disk show -shelf shelf_number`
   b. Check the output to verify that there are no aggregates on the disk drives in the disk shelves you are removing.

      Disk drives with no aggregates have a dash in the `Container Name` column.

   c. Check the output to verify that ownership is removed from the disk drives on the disk shelves you are removing.

      Disk drives with no ownership have a dash in the `Owner` column.

      > If you have failed disk drives in the shelf you are removing, they have broken in the `Container Type` column. (Failed disk drive do not have ownership.)

The following output shows disk drives on the disk shelf being removed (disk shelf 3) are in a correct state for removing the disk shelf. The aggregates are removed on all of the disk drives; therefore, a dash appears in the `Container Name` column for each disk drive. Ownership is also removed on all of the disk drives; therefore, a dash appears in the `Owner` column for each disk drive.

```
cluster::> storage disk show -shelf 3

           Usable           Disk   Container   Container
Disk         Size Shelf Bay Type   Type        Name       Owner
-------- -------- ----- --- ------ ----------- ---------- ---------
...
1.3.4           -     3   4 SAS    spare               -         -
1.3.5           -     3   5 SAS    spare               -         -
1.3.6           -     3   6 SAS    broken              -         -
1.3.7           -     3   7 SAS    spare               -         -
...
```

1. Physically locate the disk shelves you are removing.

   If needed, you can turn on the disk shelf's location (blue) LEDs to aid in physically locating the affected disk shelf: `storage shelf location-led modify -shelf-name` *`shelf_name`* `-led-status on`

   > A disk shelf has three location LEDs: one on the operator display panel and one on each IOM12 module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

2. If you are removing an entire stack of disk shelves, complete the following substeps; otherwise, go to the next step:

   a. Remove all SAS cables on path A (IOM A) and path B (IOM B).

      This includes controller-to-shelf cables and shelf-to-shelf cables for all disk shelves in the stack you are removing.

   b. Go to step 9.

3. If you are removing one or more disk shelves from a stack (but keeping the stack), recable the path A (IOM A) stack connections to bypass the disk shelves you are removing by completing the applicable set of substeps:

   If you are removing more than one disk shelf in the stack, complete the applicable set of substeps one disk shelf at a time.

   > Wait at least 10 seconds before connecting the port. The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place and the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

If you are removing…	Then…
A disk shelf from either end (logical first or last disk shelf) of a stack	a. Remove any shelf-to-shelf cabling from IOM A ports on the disk shelf you are removing and put them aside. b. Unplug any controller-to-stack cabling connected to IOM A ports on the disk shelf you are removing and plug them into the same IOM A ports on the next disk shelf in the stack. The “next” disk shelf can be above or below the disk shelf you are removing depending on which end of the stack you are removing the disk shelf from.
A disk shelf from the middle of the stack A disk shelf in the middle of a stack is only connected to other disk shelves—not to any controllers.	a. Remove any shelf-to-shelf cabling from IOM A ports 1 and 2 or from ports 3 and 4 on the disk shelf you are removing and IOM A of the next disk shelf, and then put them aside. b. Unplug the remaining shelf-to-shelf cabling connected to IOM A ports on the disk shelf you are removing and plug them into the same IOM A ports on the next disk shelf in the stack. The “next” disk shelf can be above or below the disk shelf you are removing depending on which IOM A ports (1 and 2 or 3 and 4) you removed the cabling from.

You can refer to the following cabling examples when removing a disk shelf from an end of a stack or the middle of a stack. Note the following about the cabling examples:

- The IOM12 modules are arranged side-by-side as in a DS224C or DS212C disk shelf; if you have a DS460C, the IOM12 modules are arranged one above the other.
- The stack in each example is cabled with standard shelf-to-shelf cabling, which is used in stacks cabled with multipath HA or multipath connectivity.

  You can infer the recabling if your stack is cabled with quad-path HA or quad-path connectivity, which uses double-wide shelf-to-shelf cabling.

- The cabling examples demonstrate recabling one of the paths: path A (IOM A).

  You repeat the recabling for path B (IOM B).

- The cabling example for removing a disk shelf from the end of a stack demonstrates removing the logical last disk shelf in a stack that is cabled with multipath HA connectivity.

  You can infer the recabling if you are removing the logical first disk shelf in a stack or if your stack has multipath connectivity.

4. Verify that you bypassed the disk shelves you are removing and reestablished the path A (IOM A) stack connections correctly: `storage disk show -port`

   For HA pair configurations, you run this command from the clustershell of either controller. It might take up to a minute for the system to complete discovery.

   The first two lines of output show disk drives with connectivity through both path A and path B. The last two lines of output show disk drives with connectivity through a single-path, path B.

```
cluster::> storage show disk -port

PRIMARY  PORT SECONDARY      PORT TYPE SHELF BAY
-------- ---- ---------      ---- ---- ----- ---
1.20.0   A    node1:6a.20.0  B    SAS  20    0
1.20.1   A    node1:6a.20.1  B    SAS  20    1
1.21.0   B    -              -    SAS  21    0
1.21.1   B    -              -    SAS  21    1
...
```

5. The next step depends on the `storage disk show -port` command output:

If the output shows…	Then…
All disk drives in the stack are connected through path A and path B except for the ones in the disk shelves you disconnected, which are only connected through path B	Go to the next step. You successfully bypassed the disk shelves you are removing and reestablished path A on the remaining disk drives in the stack.
Anything other than the above	Repeat Step 5 and Step 6. You must correct the cabling.

6. Complete the following substeps for the disk shelves (in the stack) you are removing:
   a. Repeat Step 5 through Step 7 for path B.

      When you repeat Step 7 and if you have recabled the stack correctly, you should only see all remaining disk drives connected through path A and path B.

   b. Repeat Step 1 to confirm that your system configuration is the same as before you removed one or more disk shelves from a stack.
   c. Go to the next step.
7. If when you removed ownership from the disk drives (as part of the preparation for this procedure), you disabled disk ownership automatic assignment, reenable it by entering the following command; otherwise, go to the next step: `storage disk option modify -autoassign on`

   For HA pair configurations, you run the command from the clustershell of both controllers.

8. Power off the disk shelves you disconnected and unplug the power cords from the disk shelves.
9. Remove the disk shelves from the rack or cabinet.

   To make a disk shelf lighter and easier to maneuver, remove the power supplies and I/O modules (IOMs).

   For DS460C disk shelves, you can also use the four detachable handles that shipped with your disk shelf. Handles (two on each side of the chassis) are installed by pushing up until they click into place. As you slide the disk shelf onto the rails, detach handles using the thumb latch.

   It is recommended that you use a mechanical hoist or lift if you are moving a fully loaded DS460C disk shelf.

   A fully loaded DS460C disk shelf can weigh approximately 247 lbs (112 kg).

Hot-swap or replace an IOM12 module - shelves with IOM12 modules

Your system configuration determines whether you can perform a nondisruptive IOM12 module hot-swap or a disruptive IOM12 module replacement when an IOM12 module fails.

Before you begin

All other components in the system—including the other IOM12 module—must be functioning properly.

About this task

- For multipathed (multipath HA or multipath) and quad-pathed (quad-path HA or quad-path) configurations, you can hot-swap an IOM12 module (nondisruptively replace an IOM12 module in a system that is powered on and serving data—I/O is in progress).
- For FAS2600 series and FAS2700 single-path HA configurations, you must perform a takeover and giveback operation to replace an IOM12 module in a system that is powered on and serving data—I/O is in progress.
- For FAS2600 series single-path configurations, you must halt your system to replace an IOM12 module.

  If you attempt to hot-swap an IOM12 module on a disk shelf with a single-path connection, you will lose all access to the disk drives on the disk shelf as well as any disk shelves beneath. You could also bring down your entire system.

- The best practice is to have the current versions of disk shelf (IOM) firmware and disk drive firmware on your system before adding new disk shelves, shelf FRU components, or SAS cables.

  Current versions of firmware can be found on the NetApp Support Site.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

- Disk shelf (IOM) firmware is automatically updated (nondisruptively) on a new IOM12 module with a non current firmware version.

  IOM firmware checks occur every ten minutes. An IOM firmware update can take up to 30 minutes.

- If needed, you can turn on the disk shelf's location (blue) LEDs to aid in physically locating the affected disk shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

  A disk shelf has three location LEDs: one on the operator display panel and one on each IOM12 module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

- If needed, you can refer to the Monitoring disk shelf LEDs section for information about the meaning and location of disk shelf LEDs on the operator display panel and FRU components.

Steps

1. Properly ground yourself.
2. Unpack the new IOM12 module, and set it on a level surface near the disk shelf.

   Save all packaging materials for use when returning the failed IOM12 module.

3. Physically identify the failed IOM12 module from the system console warning message and the illuminated attention (amber) LED on the failed IOM12 module.
4. Perform one of the following actions based on the type of configuration you have:

If you have a…	Then…
Multipath HA, multipath, quad-path HA, or quad-path configuration	Go to the next step.
FAS2600 series and FAS2700 single-path HA configuration	a. Determine the target node (the node the failed IOM12 module belongs to). IOM A belongs to Controller 1. IOM B belongs to Controller 2. b. Take over the target node: `storage failover takeover -bynode partner HA node`
FAS2600 series single-path configuration	a. Shut down the system from the system console: `halt` b. Verify that your system halted by checking the storage system console.

5. Disconnect the cabling from the IOM12 module that you are removing.

   Make note of the IOM12 module ports each cable is connected to.

6. Press the orange latch on the IOM12 module cam handle until it releases, and then open the cam handle fully to release the IOM12 module from the mid plane.

7. Use the cam handle to slide the IOM12 module out of the disk shelf.

   When handling an IOM12 module, always use two hands to support its weight.

8. Wait at least 70 seconds after removing the IOM12 module before you install the new IOM12 module.

   Waiting at least 70 seconds enables the driver to register the shelf ID correctly.

9. Using two hands, with the cam handle of the new IOM12 module in the open position, support and align the edges of the new IOM12 module with the opening in the disk shelf, and then firmly push the new IOM12 module until it meets the mid plane.

   > Do not use excessive force when sliding the IOM12 module into the disk shelf; you might damage the connectors.

10. Close the cam handle so that the latch clicks into the locked position and the IOM12 module is fully seated.
11. Reconnect the cabling.

    The SAS cable connectors are keyed; when oriented correctly into an IOM port, the connector clicks into place and the IOM port LNK LED illuminates green. You insert a SAS cable connector into an IOM port with the pull tab oriented down (on the underside of the connector).

12. Perform one of the following actions based on the type of configuration you have:

If you have a…	Then…
Multipath HA, multipath, quad-path HA, or quad-path configuration	Go to the next step.

If you have a…	Then…
FAS2600 series and FAS2700 single-path HA configuration	Give back the target node: `storage failover giveback -fromnode partner_HA_node`
FAS2600 series single-path configuration	Reboot your system.

13. Verify that the IOM12 module port links have been established.

    For each module port that you cabled, the LNK (green) LED illuminates when one or more of the four SAS lanes have established a link (with either an adapter or another disk shelf).

14. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Hot-swap a power supply - shelves with IOM12 modules

You can hot-swap a failed power supply in a DS460C, DS224C, or DS212C disk shelf.

Before you begin

All other components in the system—including the other power supply—must be functioning properly.

About this task

- If you are replacing more than one power supply, you must do so one at a time so that the disk shelf maintains power.
- You must replace a power supply within two minutes of removal to minimize disruption to the disk shelf's airflow.
- Always use two hands when removing, installing, or carrying a power supply to support its weight.
- The best practice is to have the current versions of disk shelf (IOM) firmware and disk drive firmware on your system before adding new disk shelves, shelf FRU components, or SAS cables.

  Current versions of firmware can be found on the NetApp Support Site.

  NetApp Downloads: Disk Shelf Firmware

  NetApp Downloads: Disk Drive Firmware

- If needed, you can turn on the disk shelf's location (blue) LEDs to aid in physically locating the affected disk shelf: `storage shelf location-led modify -shelf-name shelf_name -led-status on`

  A disk shelf has three location LEDs: one on the operator display panel and one on each IOM12 module. Location LEDs remain illuminated for 30 minutes. You can turn them off by entering the same command, but using the off option.

- If needed, you can refer to the Monitoring disk shelf LEDs section for information about the meaning and location of disk shelf LEDs on the operator display panel and FRU components.

Steps

1. Properly ground yourself.
2. Unpack the new power supply and set it on a level surface near the shelf.

   Save all packing materials for use when returning the failed power supply.

3. Physically identify the failed power supply from the system console warning message and the illuminated attention (amber) LED on the power supply.
4. Turn off the failed power supply and disconnect the power cable:
   a. Turn off the power switch on the power supply.
   b. Open the power cord retainer and unplug the power cord from the power supply.
   c. Unplug the power cord from the power source.
5. Press the orange latch on the power supply cam handle until it releases, and then open the cam handle to fully release the power supply from the mid plane.

   The following illustration is for a power supply used in a DS224C or DS212C disk shelf; however, the latch operates the same way for power supplies used in DS460C disk shelves.

6. Use the cam handle to slide the power supply out of the disk shelf.

   If you have a DS224C or DS212C disk shelf, as you remove the power supply, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

   When handling a power supply, always use two hands to support its weight.

7. Make sure that the on/off switch of the new power supply is in the Off position.
8. Using two hands, with the cam handle of the new power supply in the open position, support and align the edges of the new power supply with the opening in the disk shelf, and then firmly push the new power supply until it meets the mid plane.

> Do not use excessive force when sliding the power supply into the disk shelf; you might damage the connectors.

9. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
10. Reconnect the power supply cable and turn on the new power supply:
    a. Reconnect the power cord to the power source.
    b. Reconnect the power cord to the power supply and secure the power cord with the power cord retainer.
    c. Turn on the power switch.

       The power supply's power (green) LED and attention (amber) LED illuminate, and then within 40 seconds, the attention (amber) LED turns off.
11. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Monitor disk shelf LEDs - shelves with IOM12 modules

You can monitor the health of your disk shelf by understanding the location and status conditions of the LEDs on your disk shelf components.

Operator display panel LEDs

The LEDs on the disk shelf front operator display panel indicate whether your disk shelf is functioning normally or there are problems with the hardware.

The following table describes the three LEDs on the operator display panel used in DS460C, DS224C, and DS212C disk shelves:

LED icon	LED name	State	Description
	Power	Solid green	One or more power supplies are supplying power to the disk shelf.

LED icon	LED name	State	Description
!	Attention	Solid amber	An error occurred with the function of one of more FRUs: the disk shelf, disk drives, IOM12 modules, or power supplies. Check event messages to determine corrective action to take.
		Blinking amber	The shelf ID is in a pending state. Power cycle the disk shelf for the shelf ID to take affect.
	Location	Solid blue	The system administrator activated this LED function to aid in physically locating the disk shelf requiring service. The location LED on the operator display panel and both IOM12 modules illuminate when this LED function is activated. Location LEDs automatically turn off after 30 minutes.

Depending on your disk shelf model, the operator display panel looks different; however, the three LEDs are arranged in the same way.

The following illustration is of a DS224C disk shelf operator display panel with the end cap on:

IOM12 module LEDs

The LEDs on the IOM12 module indicate whether the module is functioning normally, whether it is ready for I/O traffic, and whether there are any problems with the hardware.

The following table describes IOM12 module LEDs associated with the function of the module and the function of each SAS port on the module.

The IOM12 module is used in DS460C, DS224C, and DS212C disk shelves.

LED icon	LED name	State	Description
!	Attention	Solid amber	IOM12 module function: An error occurred with the function of the IOM12 module. SAS port function: Less than all four SAS lanes established a link (with either an adapter or another disk shelf). Check event messages to determine corrective action to take.
LNK	Port link	Solid green	One or more of the four SAS lanes established a link (with either an adapter or another disk shelf).

LED icon	LED name	State	Description
	Location	Solid blue	The system administrator activated this LED function to aid in physically locating the disk shelf with the failed IOM12 module. The location LED on the operator display panel and both IOM12 modules illuminate when this LED function is activated. Location LEDs automatically turn off after 30 minutes.

The following illustration is for a IOM12 module:

Power supply LEDs

The LEDs on the power supply indicate whether the power supply is functioning normally or there are hardware problems.

The following table describes the two LEDs on power supplies used in DS460C, DS224C, and DS212C disk shelves:

LED icon	LED name	State	Description
	Power	Solid green	The power supply is functioning correctly.
		Off	The power supply failed, the AC switch is turned off, the AC power cord is not properly installed, or electricity is not being properly supplied to the power supply. Check event messages to determine corrective action to take.

LED icon	LED name	State	Description
!	Attention	Solid amber	An error occurred with the function of the power supply. Check event messages to determine corrective action to take.

Depending on your disk shelf model, power supplies can be different, dictating the location of the two LEDs.

The following illustration is for a power supply used in a DS460C disk shelf.

The two LED icons act as the labels and LEDs, meaning the icons themselves illuminate—there are no adjacent LEDs.

The following illustration is for a power supply used in a DS224C or DS212C disk shelf:

Fan LEDs on DS460C disk shelves

The LEDs on the DS460C fans indicate whether the fan is functioning normally or there are hardware problems.

The following table describes the LEDs on fans used in DS460C disk shelves:

Item	LED name	State	Description
❶	Attention	Solid amber	An error occurred with the function of the fan. Check event messages to determine corrective action to take.

Disk drive LEDs

The LEDs on a disk drive indicates whether it is functioning normally or there are problems with the hardware.

Disk drive LEDs for DS224C and DS212C disk shelves

The following table describes the two LEDs on the disk drives used in DS224C and DS212C disk shelves:

Callout	LED name	State	Description
1	Activity	Solid green	The disk drive has power.
		Blinking green	The disk drive has power and I/O operations are in progress.

Callout	LED name	State	Description
❷	Attention	Solid amber	An error occurred with the function of the disk drive. Check event messages to determine corrective action to take.

Depending on your disk shelf model, disk drives are arranged vertically or horizontally in the disk shelf, dictating the location of the two LEDs.

The following illustration is for a disk drive used in a DS224C disk shelf.

DS224C disk shelves use 2.5-inch disk drives arranged vertically in the disk shelf.

The following illustration is for a disk drive used in a DS212C disk shelf.

DS212C disk shelves use 3.5-inch disk drives or 2.5-inch disk drives in carriers arranged horizontally in the disk shelf.

Disk drive LEDs for DS460C disk shelves

The following illustration and table describes the drive activity LEDs on the drive drawer and their operational states:

Location	LED	Status indicator	Description
1	Attention: Drawer attention for each drawer	Solid amber	A component within the drive drawer requires operator attention.
		Off	No drive or other component in the drawer requires attention and no drive in the drawer has an active locate operation.
		Blinking amber	A locate drive operation is active for any drive within the drawer.
2-13	Activity: Drive activity for drives 0 through 11 in the drive drawer	Green	The power is turned on and the drive is operating normally.
		Blinking green	The drive has power, and I/O operations are in progress.
		Off	The power is turned off.

When the drive drawer is open, an attention LED can be seen in front of each drive.

1	Attention LED light on

Switches

You can use these links to find switch documentation.

- Broadcom-supported BES-53248 switches
- Nexus 9336C-FX2 cluster switches
- 9336C-FX2 shared switches
- Nexus 92300YC cluster switches
- Nexus 5596
- Nexus 3232C
- Nexus 3132Q-V
- CN1610
- CN1601

Cabinet and rail kits

SuperRail kit installation instructions

The SuperRail can be either installed on a standard square-hole four-post rack or a standard round-hole four-post rack by using the round-to-square hole adaptor brackets.

Installing SuperRail to square-hole four-post rack

Installing SuperRail to round-hole four-post rack

Two-post support rail kit installation instructions - AFF A700 and FAS9000

There are two, two-post support rail kits that can be used with the FAS9000 and AFF

A700 systems. One kit allows you to flush-mount your system in the two-post rack, and the other kit allows you to mid-mount your system in the two-post rack.

Install the two-post mid-mount rail kit

Install the two-post flush-mount rail kit

42U 1280 mm system cabinet

Prepare to install cabinet

System cabinet features

The system cabinet consists of side panels, front and rear doors, an optional bolt-down kit, an optional interconnect kit, PDUs for your equipment, and an integrated cable management system.

Feature	Description
Side panels	System cabinets have lockable, removable, and interchangeable side panels.
Perforated front and rear doors	System cabinets have removable front and rear doors with a quick release mechanism. The front door is reversible, and the rear doors are split. Both doors are perforated for cooling.
Common key	This key unlocks the front doors, rear doors, and side panels.
Spares kit	This kit is inside the system cabinet, attached to the cabinet door. It contains the following components: • Four 10-32 x 0.75 inch Phillips pilot screws • Four 10-32 cage nuts • One cage nut insertion tool • Two master key copies
Cable access	Cable pass-throughs are built into the top and bottom of the cabinet, as well as between the bottom of the rear door and the frame.
Cable management	Cable management hook and loop strapping is attached to the frame of the system cabinet at equal intervals.
Support rails	The number of support rails you receive depends on your configuration. The empty system cabinet is shipped with no support rails installed. • For configured system cabinets, one fixed rail kit is shipped with the system cabinet to support the 80xx, FAS8200, and DS4486 rear hold-down brackets. • Quick-ship system cabinets do not include the additional fixed rail kit.
Blanking panels	The number and size of blanking panels you receive depends on your configuration. The empty system cabinet is shipped with no blanking panels installed.
Bolt-down kit	This optional kit enables you to secure the system cabinet to the data center floor. The kit it is not intended for seismic stability. • Four bolt-down brackets • Four spacer brackets • Six M8x20 mm hex head bolts and washers

Feature	Description

Interconnect kit	This optional kit enables you to connect multiple system cabinets to each other.
	• Interconnect brackets
	  ◦ One set of four interconnect brackets for connecting the system cabinets with side panels on
	  ◦ One set of four interconnect brackets for connecting the system cabinets with the side panels off
	• Four M12x20 Torx-30 screws used in system cabinet with side panels on.
	• Eight M6x10 countersunk Torx-30 screws used in system cabinet with side panels off.

Support rail kit	If you ordered additional support rails with your system cabinet, each kit contains one left and one right support rail. ⓘ The support rails and kit are designed to fit only the NetApp 42U 1280 mm system cabinet. Do not use the rails or a rail kit from other system cabinets because they are not designed for use in the 42U 1280 mm system cabinet. • A left and right support rail • Two screws per rail for securing the rail to the system cabinet frame
Crescent wrench	The crescent wrench is used to remove the hold-down brackets on the packing pallet, adjust the system cabinet leveling feet, and install the bolt-down kit brackets, if ordered.

Required tools and equipment

Before unpacking and installing on your system cabinet, you should gather the necessary tools and equipment to move the system cabinet into place and install it or to perform maintenance on it.

- The appropriate hardware guide for your disk shelves
- The appropriate installation and setup instructions for your system

  All Flash FAS Documentation Resources

  FAS Storage Systems documentation resources

- #1 and #2 Phillips screwdrivers
- Torx driver for system cabinet screws
- Leveling tool for leveling the system cabinet

Space requirements and system cabinet dimensions

When unpacking your system cabinet, you must make sure that you have enough room to remove the system cabinet from the packing material. Also make sure that the intended location for the system cabinet is large enough for you to move the cabinet into place.

Required space for unpacking the system cabinet

The following table defines the requires space needed to unpack and install your system cabinet:

Dimensions	U.S.
Metric	Shipping ramp length
80 in.	203.2 cm
Clearance beyond the ramp for cabinet mobility	72 in.
182.9 cm	Shipping pallet depth
59 in.	149.9 cm
Shipping pallet width	42 in.
106.6 cm	Shipping pallet and packaging height
86 in.	218.4 cm
Total rack space, 42U	73.5 in.
186.7 cm	Rail load capacity
Supports all current systems	Supports all current systems
Empty weight	~400 lbs (~181 kg) lbs
~ 181 kg	Fully loaded ship weight
Up to 1,800 lbs	Up to 816.5 kg
Fully loaded static weight	Up to 2,700 lbs
Up to 1,224.7 kg	Front service clearance
47.2 in.	120 cm

Dimensions	U.S.
Rear service clearance **Note:** The rear door is split. Actual minimum rear clearance is approximately 1/2 the recommendation.	30 in.
76.3 cm	Minimum side clearance for panel removal
24 in.	61 cm
Minimum top clearance	12 in.

System cabinet exterior dimensions

The following illustration shows the front, rear, and side views of the system cabinet:

The following illustrations show top and bottom views of the system cabinet, and identify the openings through which you can run cable bundles from the floor of your data center into the system cabinet. The illustrations also show the location of the system cabinet casters and leveling feet.

CAUTION:

To prevent your system cabinet from falling through the data center floor, do not attempt to roll the system cabinet over a floor opening that is wider than the cable access opening at the bottom of the system cabinet.

Supported PDU types and specifications

The system cabinet supports different Power Distribution Unit (PDU) types. The PDUs are compliant with NEMA or IEC.

The most current information for PDUs supported in your system cabinet is listed in the Hardware Universe.

hwu.netapp.com

Unpack the system cabinet

You must remove the packing material that surrounds your system cabinet before you move it into place. You should also recycle the packing material after the cabinet is unpacked.

Install cabinet

Install a system cabinet

You can order a system cabinet with NetApp storage controllers and disk shelves installed in it or an empty system cabinet if you already have NetApp equipment. Several system cabinets can be connected together by using the optional interconnect kit, and they can be anchored to the data center floor by using the optional bolt-down kit.

Install the cabinet interconnect kit

You can connect system cabinets together by using the optional cabinet interconnect kit. It is recommended that you install the kit to prevent the cabinets from pulling apart and damaging system cables.

1. Place the system cabinets close together.

   The cabinets should be arranged similarly to the following illustration, with the cabinet with the controller modules in the middle, and the cabinets with additional disk shelves on either side. The sides of the cabinets should be close, but do not need to touch each other yet.

2. If you are installing the interconnect kit with the side panels on as recommended, reinstall the side panels that were removed during unpacking:
   a. Lift the side panel, tilting it about 15 degrees away from the system cabinet bottom, and then hang it over the lip at the top of the system cabinet frame.
   b. Gently push the side panel against the cabinet frame, and then lock it in place with the key.
   c. Repeat these substeps for the remaining side panels.
3. If you are installing the interconnect kit with the side panels removed, remove the front door whose hinges are on the edge where the cabinets meet:
   a. Unlock and open the front door that is being removed.

b. Use the following illustration for reference to unplug the power to the illuminated bezel:

1	
Illuminated bezel circuit board and cable	
2	
Back panel and thumbscrews	

c. Use the following illustration for reference to remove the front door:

1	
Door grounding cable	
2	
Door top hinge	
3	
Hinge pin	

Make sure that you set the removed doors in a safe place so that they are not accidently damaged.

4. Remove the rear door whose hinges are on the edge where the cabinets meet:
   a. Unlock and open the rear door that you are removing.
   b. Lift the top hinge pin until it clears the bottom of the hinge.
   c. Gently tip the top of the door away from the system cabinet frame, and then release the hinge pin.
   d. Lift the door off the bottom hinge, and then set the door aside.

5. Move the system cabinets completely together, and then align and level them by adjusting the four leveling feet at the bottom of the system cabinets.
6. Install the interconnect brackets.
   - Use the following illustration for reference if you are installing the interconnect brackets with the system cabinet side panels on, as recommended:

❶	
Plastic push-in rivets on the system cabinet top	
❷	

Top interconnect bracket	
❸	
Bottom interconnect bracket	

- Use the following illustration for reference if you are installing the interconnect brackets with the system cabinet side panels off:

7. Repeat the process for any remaining system cabinets.
8. Tighten all interconnect bracket screws.

Install the bolt-down kit

You can secure the system cabinet to the floor by installing the optional bolt-down kit. Installing the kit prevents the system cabinets from being rolled out of position.

You must supply the appropriate anchor bolt for your floor for each bolt-down bracket.

1. Mark the area on your floor where the system cabinet will be installed, and then roll the cabinet into place.

1	
Front and rear bolt-down brackets	
2	
Location of floor anchor point on the bracket	

2. Mark the anchoring points where the rear bolt-down brackets will be anchored to the floor, and then drill the holes for the brackets.

   Be sure to use the appropriate bolt sizes and type for your floor.

3. If the bolt-down brackets are too low to align with the mount points on the system cabinet frame, place a spacer bracket over the hole in the floor.
4. Loosely bolt the rear brackets to the floor, and then using the kit bolts, bolt the brackets to the cabinet frame.
5. Mark the anchoring points where the front bolt-down brackets will be anchored to the floor, and then drill the holes for the brackets.

6. If the bolt-down brackets are too low to align with the mount points on the system cabinet frame, place a spacer bracket over the hole in the floor.
7. Bolt the front brackets to the floor, and then using the kit bolts, bolt the brackets to the cabinet frame.
8. Lower the leveling feet as needed, and then tighten the rear bolt-down brackets to the floor.

Install additional support rails

Your system cabinet has some support rails already installed in it. If you need additional support rails for your system, you must install them before installing your system components.

This task applies to all controller and disk shelves except the DS212C and the DE212C disk shelves. Use the instructions in the rail kit flyer applicable to those two disk shelves.

Installing a DE212C or DS212C Shelf in a Two-Post or Four-Post Rack

1. Determine how much space your equipment requires.

   Calculate the amount of U space (1.75 inches per U) the equipment requires, based on the equipment height, and then determine where the equipment will be installed in the system cabinet based on available space.

2. Locate where you need to install the support rails, and then install them using the following illustration for reference:

3. If your equipment mounting flanges extend beyond the screw holes in the support rail, install cage nuts above the support rail, where needed.

Install equipment in the system cabinet

After you have installed any additional support rails into the system cabinet, you can add more system components to your prepopulated system cabinet or add your existing system components to an empty system cabinet.

1. Unlock and open the rear doors of the system cabinet and the front door, if it is not already open.
2. Install your equipment into the system cabinet as described in the installation instructions accompanying your equipment.

   The storage controllers should be in the middle of the system cabinet. The disk shelves should be above and below the storage controllers. Any switches should be at the very top of the system cabinet.

   > If your equipment mounting flanges extend beyond the screw holes in the support rail, install cage nuts above the support rail where needed to secure the equipment to the cabinet upright.

3. Install blanking panels over any empty bays in the system cabinet.

   If you receive the system cabinet with equipment already installed, you must remove the tie-down rails on top of the equipment that is directly below empty cabinet bays, as shown in the following illustration:

4. Reinstall the front and rear system cabinet doors.

Power on the system cabinet

You must connect the system components to the PDUs, route the PDU cables to the AC power sources, connect them to the power sources, and power on the system.

You must have separate power circuits available for each PDU in your system cabinet.

1. Connect your equipment to the PDUs, making sure that you connect each component's power supplies to a PDU on opposite sides of the system cabinet.
2. Feed the PDU power cables through an opening in the system cabinet.

   Use one of the following openings:

   - The top of the system cabinet
   - Between the rear door bottom and frame of the system cabinet
   - Through the floor opening and under the system cabinet
3. Turn off the power switches or circuit breakers on the PDUs.
4. Plug each PDU power cable into individual AC power sources that are on separate AC circuits.
5. Turn on the power switches or circuit breakers to the PDUs.
6. Turn on the power to your components, and then boot the system.
7. Close and lock the system cabinet doors.

Replace PDUs

You can replace a failed PDU in your system cabinet or replace an existing PDU with a different type of PDU.

The replacement PDU must be supported by your system cabinet and must provide sufficient power to the installed equipment.

hwu.netapp.com

1. Turn off the circuit breakers on the target PDU, and then unplug the old PDU from the AC power source.
2. Ground yourself to the system cabinet, and then unplug the power cords from each of the system components and from the PDU.
3. Remove the screws from the PDU frame, bottom screw first.

   Ensure that you support the PDU with one hand while you remove the last screw from the top of the PDU. This prevents the PDU from dropping or falling toward you after the screw is removed.

4. Remove the old PDU from the system cabinet.

   Make sure that you keep track of the mounting screws so that you can reuse them when installing the replacement PDU.

5. Remove the brackets from the old PDU, and then install them on the back of the replacement PDU.
6. While supporting the replacement PDU, align the slot on the mounting bracket of the PDU with the top holes of the frame on the inside of the system cabinet, and then secure the PDU to the system cabinet frame using the mounting screws from the old PDU.
7. Secure the bottom of the PDU to the system cabinet frame, and then tighten all of the mounting screws.
8. Verify that all of the power switches or circuit breakers are in the Off position.

   If the circuit breakers are not in the Off position, push a small screwdriver or straightened paper clip into the slot to the right of the Off label to trip the circuit breaker and turn off the circuit.

9. Plug the system power cords into the PDU, plugging each component into the PDU outlet directly across from the component.

   A best practice is to distribute the total load across the PDU branches, making each branch load as equal as possible.

10. Lock each component power cable plug in place with the cable retainer clip above it by sliding the curved edge of the cable retainer clip over the plug shoulder.
11. Plug the PDU power cord into the AC power source.
12. Turn on the PDU power switches or PDU circuit breakers.

    For PDU circuit breakers, the button is on when it is flush with the PDU frame.

Reverse cabinet front door

Reverse the system cabinet front door

You can change the direction the front door opens by removing the illuminated badge, door, top hinge, and related hardware, and then installing them on the opposite side of the front of the system cabinet frame.

You need the following tools and equipment to complete the door reversal for system cabinets with illuminated badges:

- A Phillips screwdriver
- A 5-mm Allen wrench; magnetic Allen wrench is recommended
- Needle-nose pliers
- A step ladder so that you can easily access the Allen bolts in the top hinge

Remove the illuminated badge

Removing the illuminated badge requires that you open the system cabinet front door, unplug the power cord from the back of the badge, and then remove the badge components from the system cabinet door.

Use the following illustration along with the following

steps:

1. Unlock and open the system cabinet front door.
2. Loosen the captive screws on the badge back panel on the inside of the door, and then gently pull the back panel away from the door mesh.
3. Unplug the power cord from the back panel by pressing the locking clip on the plug, unplugging the cord from the socket, and removing the cable from the back panel.

   Set the back panel aside.

4. Carefully remove the screws from the back of the badge.

   > The stems on the thumbscrews are very short. Place your free hand under the screw to catch the thumbscrew if you drop it.

5. Remove the badge from the front of the door and set it aside.

Remove the system cabinet door

You must remove the system cabinet door and side panels to move the illuminated badge and components, and to reverse the door.

1. Open the system cabinet door if it is not already open.
2. Perform the appropriate action depending on whether your cabinets are connected with the interconnect kit.

If your system cabinet is…	Then…
Not connected to another system cabinet	Go to the next step.
Connected to another system cabinet with an interconnect kit	Remove all four interconnect kit brackets and set the brackets and screws in a safe place.

3. Unlock both side panels, disconnect the grounding wires from the side panels, and then remove them and set them aside.
4. Disconnect the grounding wire from the grounding spade located at the top of the door.
5. Unscrew the grounding lug and wire assembly from the system cabinet frame and set it aside.
6. Unscrew the grounding lug assembly from the system cabinet door and set it aside.
7. Lift the top hinge pin until it clears the bottom of the hinge.
8. Gently tip the top of the door away from the system cabinet frame, and then release the hinge pin.
9. Lift the door off the bottom hinge, and set the door aside.

Move the badge power supply and cabling

You must move the power supply and illuminated badge cabling to the opposite side of the system cabinet frame before you reverse the door and reinstall the illuminated badge.

You must have removed the system cabinet door and side panels.

You must move the illuminated badge power supply, power cable, and cabling conduit to the opposite side of the system cabinet when you reverse the system cabinet door. The assembly is designed so that the cable to the badge is on the side of the cabinet where the door hinge is installed.

1. Open the power cable retaining clip, and then disconnect the power cable from the power supply.
2. Remove the power supply housing and power supply, using the illustration for reference:

a. Lift the retaining pin on the power supply housing, and then remove the housing cover by rotating it downward and lifting it off the rear power supply housing.

> The power supply is attached to the power supply housing with a hook and loop patch.

b. Disconnect the power supply from the illuminated badge cable, and then set the power supply and power supply cover to the side.

c. Remove the screws from the top and bottom of the power supply housing that is attached to the system cabinet frame, and then remove the power supply housing.

3. Install the power supply and power supply housing on the opposite side of the system cabinet:

a. Locate the two screw holes next to each other on the cabinet frame, and then attach the top of the power supply housing to the bottom-most of the two screw holes.

> You might need to remove the bottom cable retention strap, if present.

b. Secure the bottom of the power supply housing to the system cabinet frame.

c. Install the power supply cover and power supply by aligning the cover hooks with the power supply back, pulling the plunger up on the cover, rotating the plunger closed, and then releasing the plunger.

4. Remove the bezel power supply conduit by removing the conduit retaining clips from the retaining clips, and then slide the conduit off the power cable.

Keep the retaining clips and screws for installing the conduit on the opposite side of the cabinet.

5. Move the badge power cable to the other side of the cabinet:

a. Rotate the rubber cable retainer on the cabinet upright 180° to the right, remove it from the system cabinet frame, and then gently pull the cable out of the system cabinet.

b. Move the cable to the other side of the cabinet, and then thread it completely through the hole near the top of the cabinet upright.

c. Align the rubber cable retainer with the hole in the frame, push it in as far as it will go, and then rotate the cable retainer 180° to the left to secure it.

d. Run the cable along the cabinet frame to the back of the cabinet.

6. Reinstall the cable conduit:

   a. Slide the conduit over the PDU power cable and route the conduit along the system cabinet frame to the PDU.

   b. Install the conduit retaining clips from the other side of the cabinet over the conduit to secure it to the cabinet frame.

7. Plug the badge cable back into the power supply, but do not reconnect the power supply to the power source.

Reverse the door hinge and lock catch

When reversing the system cabinet door, you must move the system cabinet door hinge and lock catch to the opposite front-side system cabinet upright.

You need the following tools:

- Phillips screwdriver
- 5 mm Allen wrench; magnetic Allen wrench is recommended
- Needle-nose pliers
- Step ladder so that you can easily access the Allen screws in the top hinge

1. Remove the screws securing the top hinge from the system cabinet frame, and set the screws and hinge aside.

   > Be careful when removing the Allen screws to avoid dropping them into the cabinet frame. Spare Allen screws are provided in the spares kit that shipped with your system cabinet.

2. Remove the screws securing the bottom hinge from the system cabinet frame, and set the screws and hinge aside.

1	
Door grounding screw with grounding wire spade	
2	
Grounding wire	
3	
Frame grounding wire lug	
4	
Top front door hinge with hinge pin held by retaining clip	
5	
Lock catch	

3. Reverse the hinge pin from the top hinge:
   a. Lift the hinge pin and expose the retaining clip on the hinge pin shaft.

b. Using the needle-nose pliers, gently remove the retaining clip from the hinge pin shaft and set it aside.
c. Slide the hinge pin and spring out of the hinge body.
d. Rotate the hinge so that the thread holes are facing the opposite side of the hinge, and then install the hinge pin and spring back into the hinge.
e. Install the hinge retaining clip onto the hinge pin.

   Make sure that you push the retaining clip completely onto the hinge pin.

4. Reinstall the hinges:
   a. Insert the top Allen screw through the system cabinet upright, aligning it with the top threaded hole on the top hinge, and then partially tighten the Allen screw.

      Do not completely tighten the screw until after the second Allen screw is installed.

   b. Insert the bottom Allen screw through the system cabinet upright, aligning it with the bottom threaded hole on the top hinge, and then partially tighten the Allen screw.
   c. Tighten the top and bottom Allen screws.
   d. Repeat these steps for the bottom hinge.
5. Remove the screws from the lock catch, and then move the lock catch to the opposite front-side system cabinet upright.
6. Rotate the catch 180 degrees, and then secure it to the system cabinet upright.

Reinstall the door and illuminated badge

After you move the power supply and components to the other side of the system cabinet and moved the hinges and lock catch, you must reinstall the system cabinet door and the illuminated badge, and then reconnect the badge to the power source.

Reinstall the system cabinet door

After you reverse the door hinge and door catch, you must reinstall the grounding wire and lug assembly and wire, and the system cabinet front door prior to reinstalling the illuminated badge.

1. Rotate the door 180 degrees.
2. Align the bottom of the door with the bottom hinge post, and then seat the door bottom on the hinge post.
3. Lift the top hinge pin so that it clears the hinge housing.
4. Tip the top of the door into the hinge housing so that the hinge pin and door hinge are aligned, and then release the hinge pin.

   Make sure that the hinge pin is seated completely through the door hinge and the bottom of the door hinge housing.

5. Reattach the grounding lug and wire assembly to the system cabinet frame on the same side of the newly reversed front door and reinstall the grounding lug with spade on the top of the system cabinet door.
6. Reattach the grounding wire to the spade on the grounding lug assembly on the system cabinet door.

7. Reinstall either the side panels or the interconnect brackets, as applicable:
    - If your system cabinet is not connected to another system cabinet, reinstall the side panels.
    - If your system cabinet is connected to another system cabinet with an interconnect kit, reinstall the interconnect brackets.

Reinstall the illuminated badge

After the system cabinet door is installed, you need to install the illuminated badge to complete the door reversal process, and then close and lock the front door.

1. Using the following illustration for reference, reinstall the illuminated badge on the front door of the system cabinet:

2. Close and lock the front door.

Other models

You can use these links to find documentation for other AFF and FAS platforms.

Platform models

AFF 8000 Series documentation

FAS8000 Series documentation

FAS6200 Series documentation

FAS3200 Series documentation

FAS2500 Series documentation

FAS2200 Series documentation

Shelf models

DS2246 disk shelf documentation

DS4486 disk shelf documentation

DS4246 disk shelf documentation

DS4243 disk shelf documentation

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for disk shelves

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.