∩ NetApp

FAS500f systems

ONTAP Systems

NetApp
February 17, 2022

Table of Contents

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.

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.

(i) 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.

(i) 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 .

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

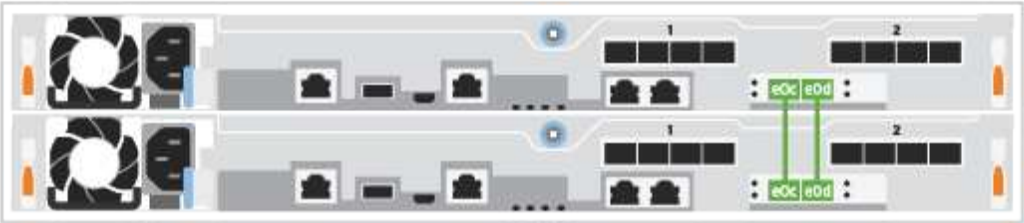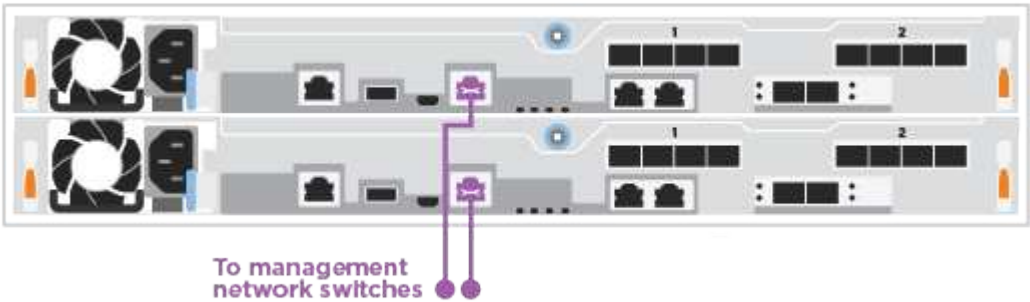Contact your network administrator for information about connecting the system to the switches.

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

> ℹ️ 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.
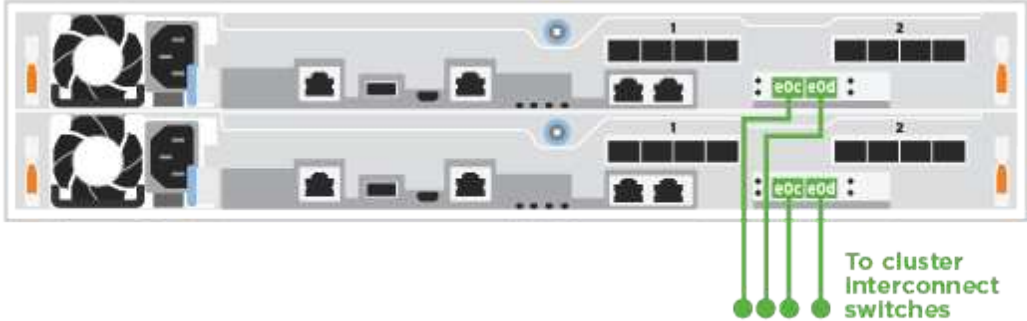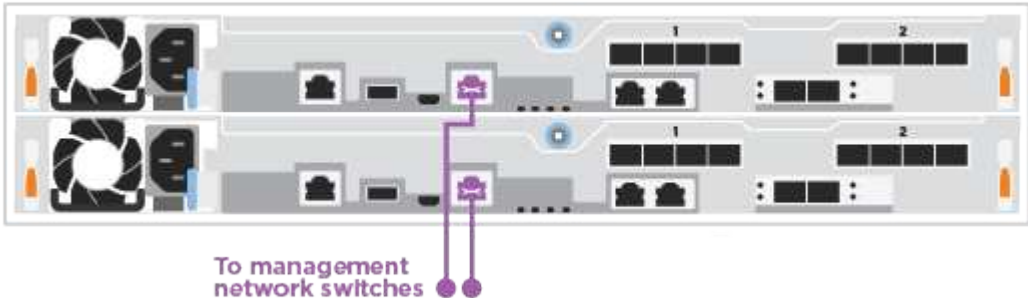

> ⓘ As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

+

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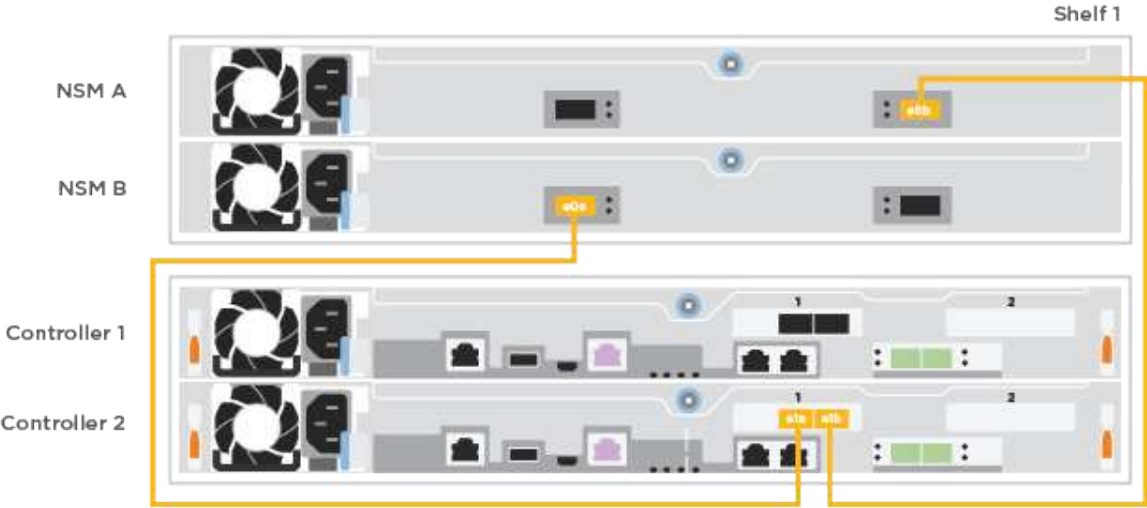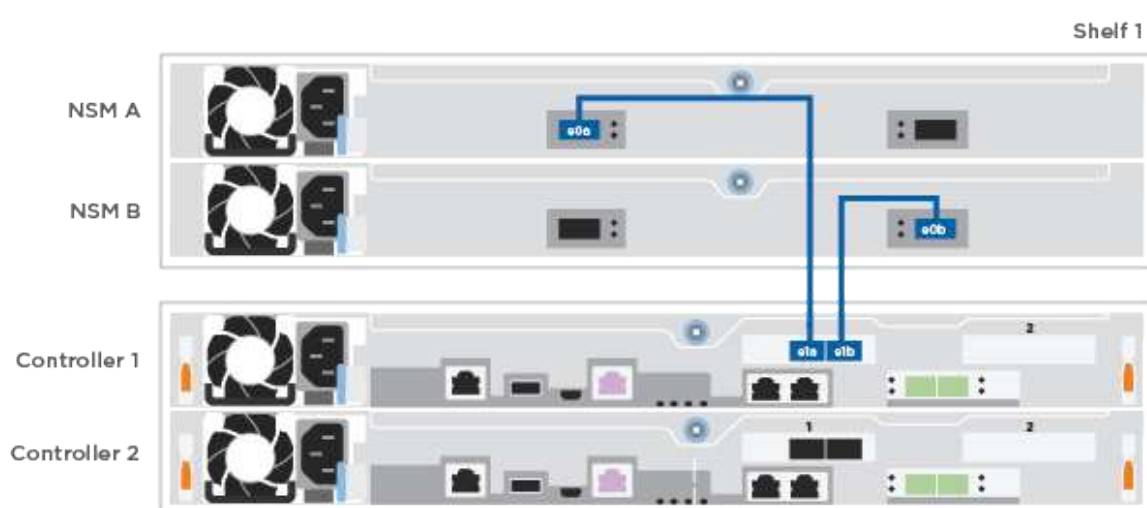
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

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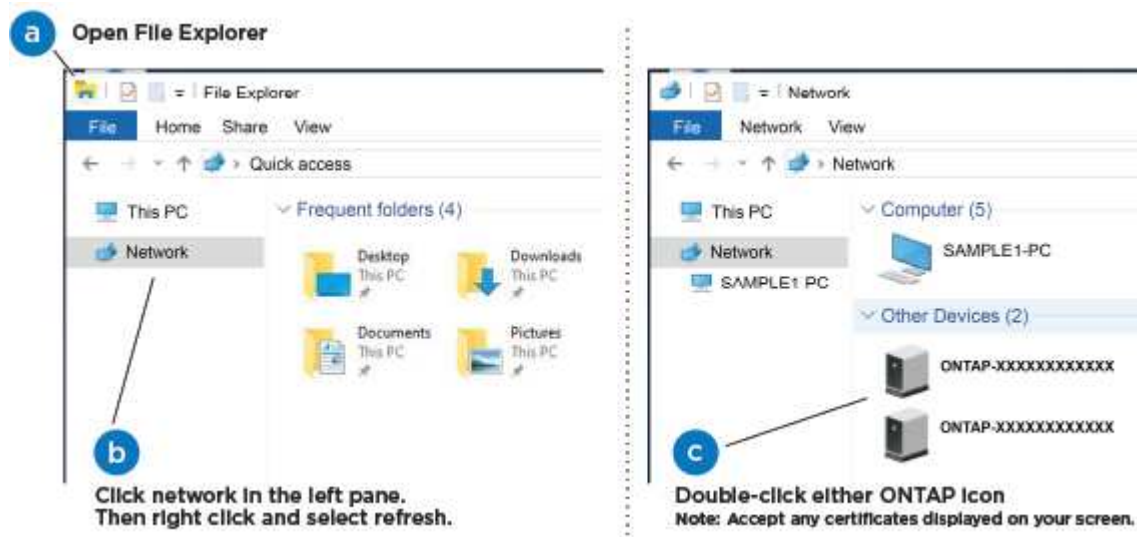
   a. Open File Explorer.
   b. Click **Network** in the left pane.
   c. Right-click and select **refresh**.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > (i) 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.

> ℹ️ 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. > ℹ️ 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.

> ℹ️ 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

Replace the boot media - 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 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 as needed - FAS500f

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

Prior to shutting down the impaired node and checking the status of the onboard encryption keys, you must check the status of the impaired node, 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; see the NetApp Encryption overview with the CLI.

Steps

1. Check the status of the impaired node:
   - If the impaired node is at the login prompt, log in as `admin`.
   - If the impaired node is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy node.
   - If the impaired node 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 node if up, or on the partner node if the impaired node 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 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`

Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired node, 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 node.

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 node.

   - 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 node.

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 node.

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 node.

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 node.

- 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 node.

  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 node.

  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 node.

Shut down the node - FAS500f

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

Option 1: Most configurations

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

Steps

1. If the impaired node isn't at the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node shows Waiting for giveback…, press Ctrl-C, and then respond y. +

2. 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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node shows Waiting for giveback…, press Ctrl-C, and then respond `y`. +

Remove the controller module, replace the boot media and transfer the boot image to 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.

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 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.

❶	Remove the screw securing the boot media to the motherboard in the controller module.
❷	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.

1	Controller module cover
2	Thumbscrew

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

9. 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. 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.

16. Check the boot environment variables:

   ◦ `bootarg.init.boot_clustered`

   ◦ `partner-sysid`

   ◦ `bootarg.init.switchless_cluster.enable`

17. 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>`

18. 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>`

19. Save the environment variables you changed with the **`savenv`** command

20. Confirm your changes using the **`printenv`** **`variable-name`** command.

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 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.

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 node.

2. Use the `boot_ontap` command at the LOADER prompt to boot the node.

3. Check the console output:

If the console displays…	Then…
The LOADER prompt	Boot the node to the boot menu: `boot_ontap menu`
Waiting for giveback….	a. Enter `Ctrl-C` at the prompt 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

> (i) 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-------------------------
TmV0QXBwIEtleSBCCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1lWgE5DLRqkiAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAIAAAAAAAgAZJElWvdeHr5RCAvHGclo+wAAAAAAAAA
IgAAAAAAAoAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAA
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 node and login as "admin".

9. Confirm the target node 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 node.

    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 node.

14. Give back the target node 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 node and port.

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

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

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

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target node.

2. Use the `boot_ontap` command at the LOADER prompt to boot the node.

3. Check the console output:

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

4. Move the console cable to the partner node and give back the target node storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.

   ◦ If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.

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

   > (i)   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 node and port.

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

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

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

9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

10. Use the `security key-manager key query` command to display the 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.

> ℹ️ If the command fails, contact Customer Support.

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

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

11. Connect the console cable to the partner node.

12. Give back the node using the `storage failover giveback -fromnode local` command.

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

Return the failed part to NetApp - 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

Replace the chassis - 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 node or nodes in the chassis prior to moving them to the new chassis.

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 node shows `false` for eligibility and health, you must correct the issue before shutting down the impaired node; 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 nodes in the cluster	`cluster ha modify -configured false storage failover modify -node node0 -enabled false`
More than two nodes in the cluster	`storage failover modify -node node0 -enabled false`

2. Halt the node, 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 node "node-name" to be marked as
   unhealthy. Unhealthy nodes do not participate in quorum voting. If the
   node goes out of service and one more node 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}:
   ```

   > (i) 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 node and start from the beginning of this procedure. If repeated attempts to cleanly shut down the node fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second node 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 - FAS500f

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).

❶	Lever
❷	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. 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.

   > ℹ️ 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 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.

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

Replace the controller module - 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 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 module - FAS500f

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

To shut down the impaired node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node shows Waiting for giveback…, press Ctrl-C, and then respond `y`. +

Option 2: Controller is in a MetroCluster

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

To shut down the impaired node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node shows Waiting for giveback…, press Ctrl-C, and then respond `y`. +

Replace controller module - FAS500f

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

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.
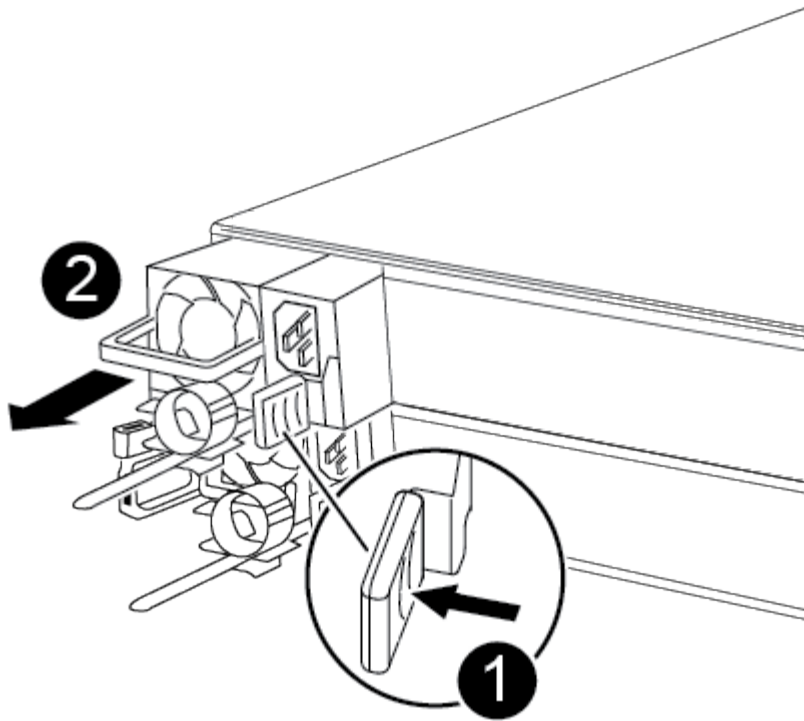
1	Blue power supply locking tab
2	Power supply

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.

❶	Remove the screw securing the boot media to the motherboard in the impaired controller module.
❷	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.

❶	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.

❶	Squeeze the clip on the face of the battery plug.
❷	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.

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.

❶	Controller module cover
❷	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.

> ℹ️ 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.

> ℹ️ 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 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.

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 node 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* 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:

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.

> (i)   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
 .
 .
 .
```

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 - 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 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 - 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

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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode `*`impaired_node_name`* + When the impaired node 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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify –node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

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

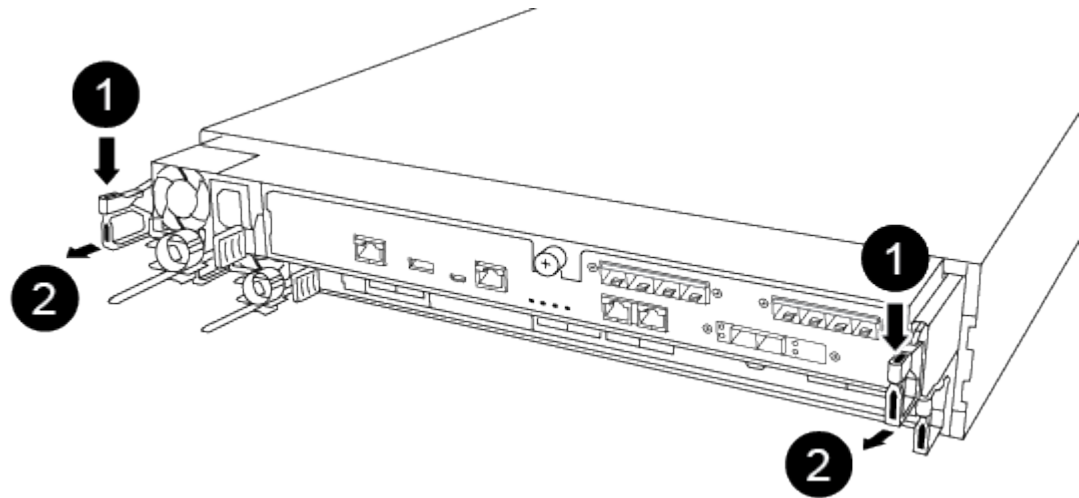## Step 2: Remove the controller module

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.

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

①		Lever
②		Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

❶	Thumbscrew
❷	Controller module cover.

7. Lift out the air duct cover.

Step 3: Replace a DIMM

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

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

Replacing a DIMM

1. Replace the impaired DIMM on your controller module.

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

   > ℹ️   The fault LED located on the board next to each DIMM blinks every two seconds.
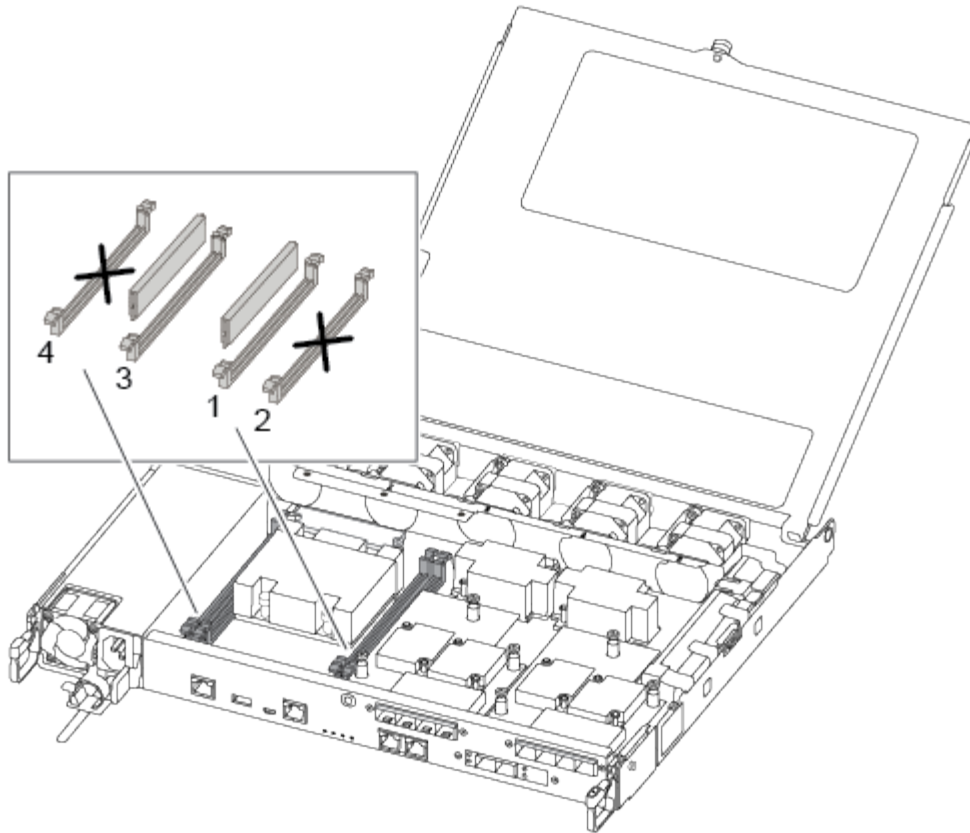
2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.

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.
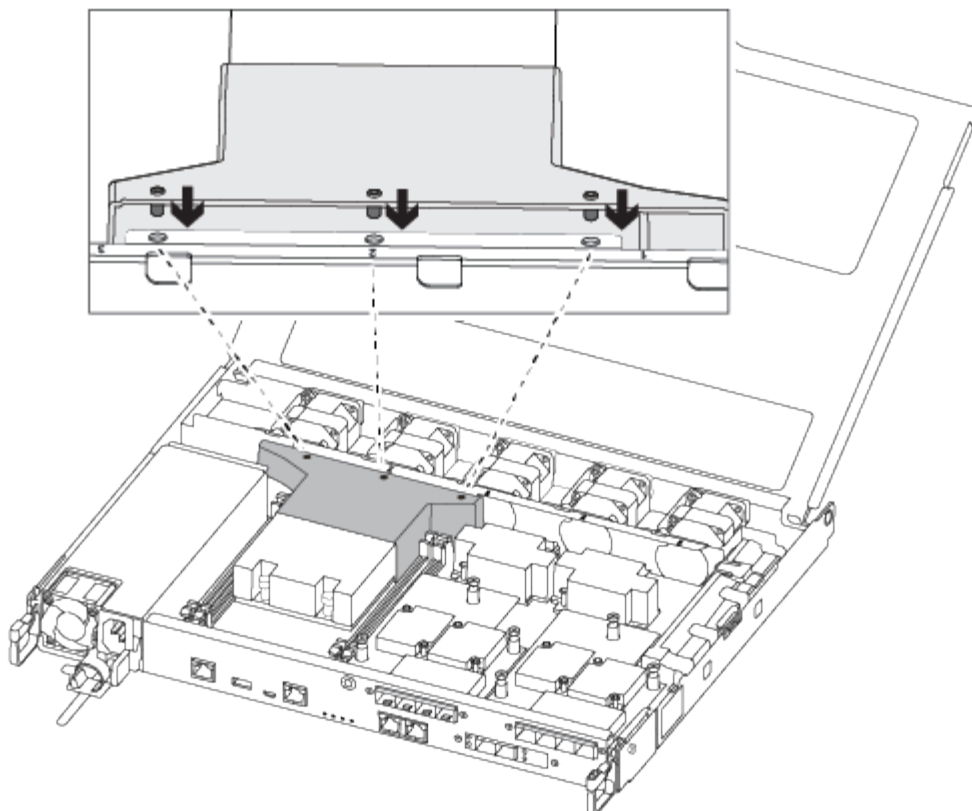
2. Close the controller module cover and tighten the thumbscrew.
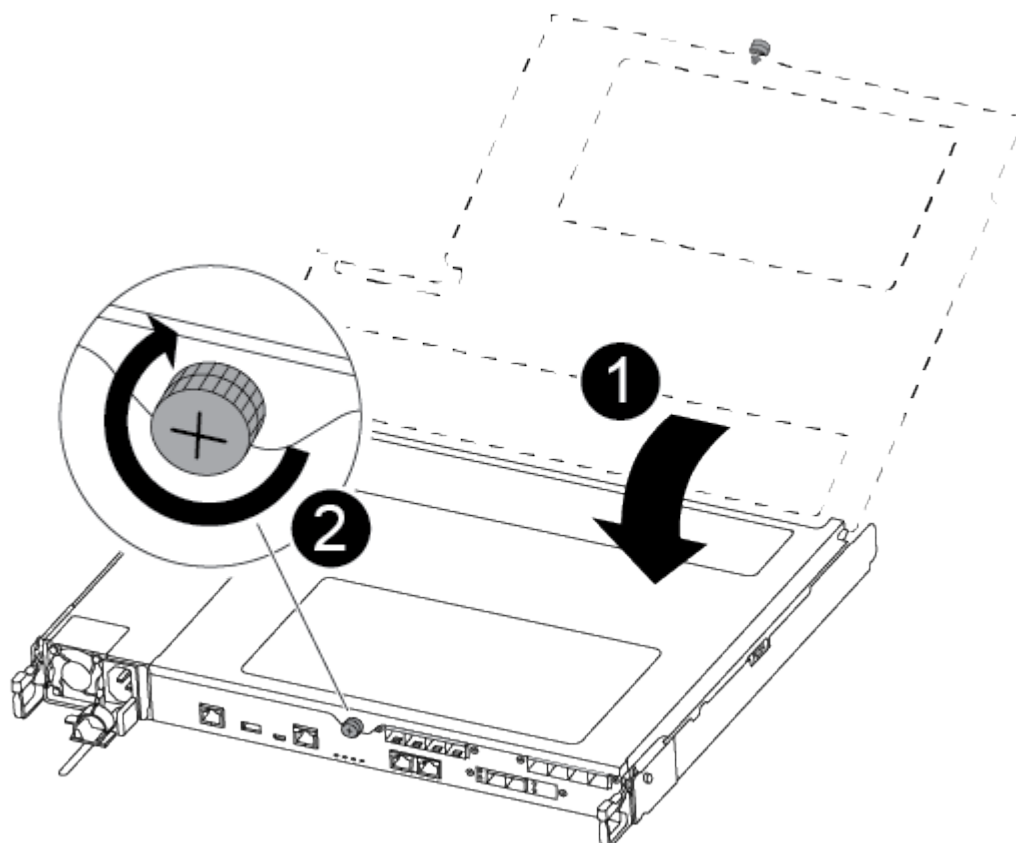
1	Controller module cover
2	Thumbscrew

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 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 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 fan — FAS500f

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

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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify –node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired node from the healthy node: `storage failover takeover -ofnode` *`impaired_node_name`* + When the impaired node 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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node shows Waiting for giveback…, press Ctrl-C, and then respond `y`. +

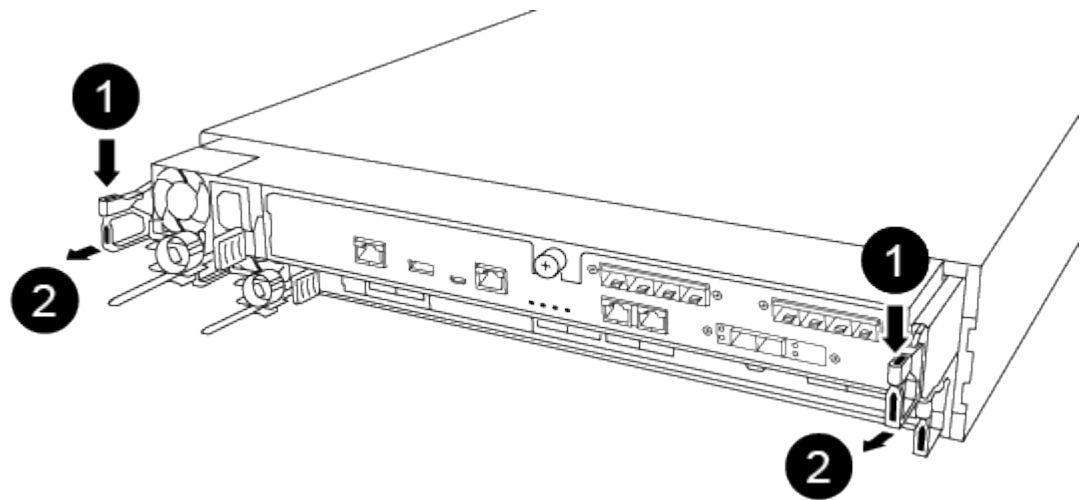## Step 2: Remove the controller module

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).

❶	Lever
❷	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat,

stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

❶	Thumbscrew
❷	Controller module cover

Step 3: Replace 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.
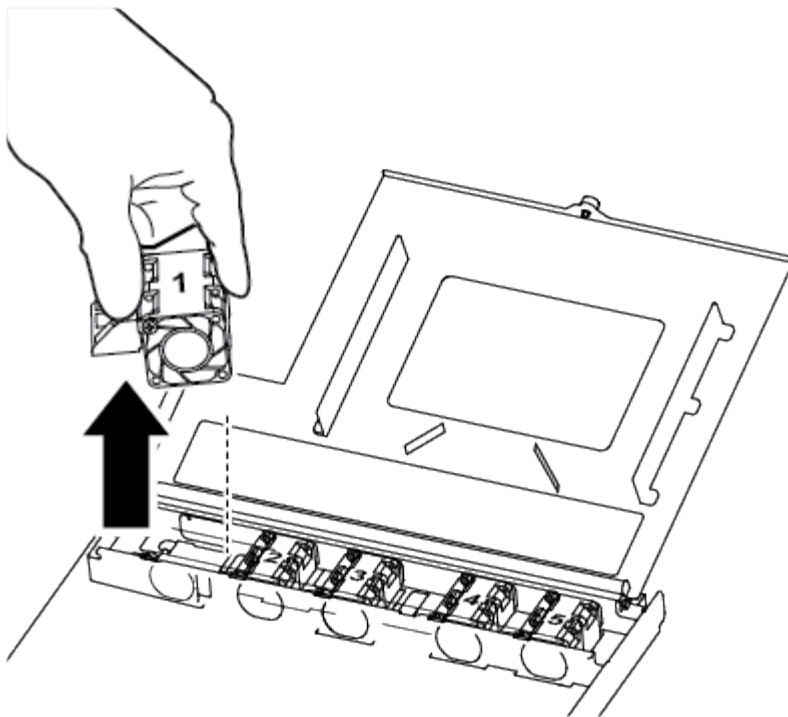
①	Fan module

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.

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 node 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

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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify –node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node 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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

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

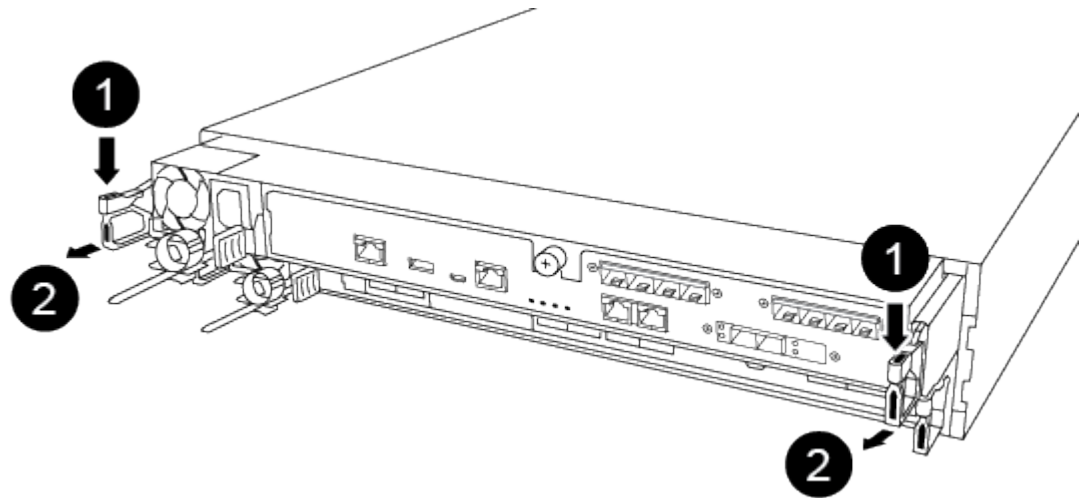| If the impaired node is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired node from the healthy node: `storage failover takeover -ofnode` *impaired_node_name* + When the impaired node shows Waiting for giveback…, press Ctrl-C, and then respond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

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

❶	Lever
❷	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

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 node 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

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 node, you must determine the status of the node and, if necessary, take over the

node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify –node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node 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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode` *impaired_node_name* + When the impaired node 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.

> (i) 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.

   ℹ️ It is recommended that you follow the illustrated instructions in the order listed.
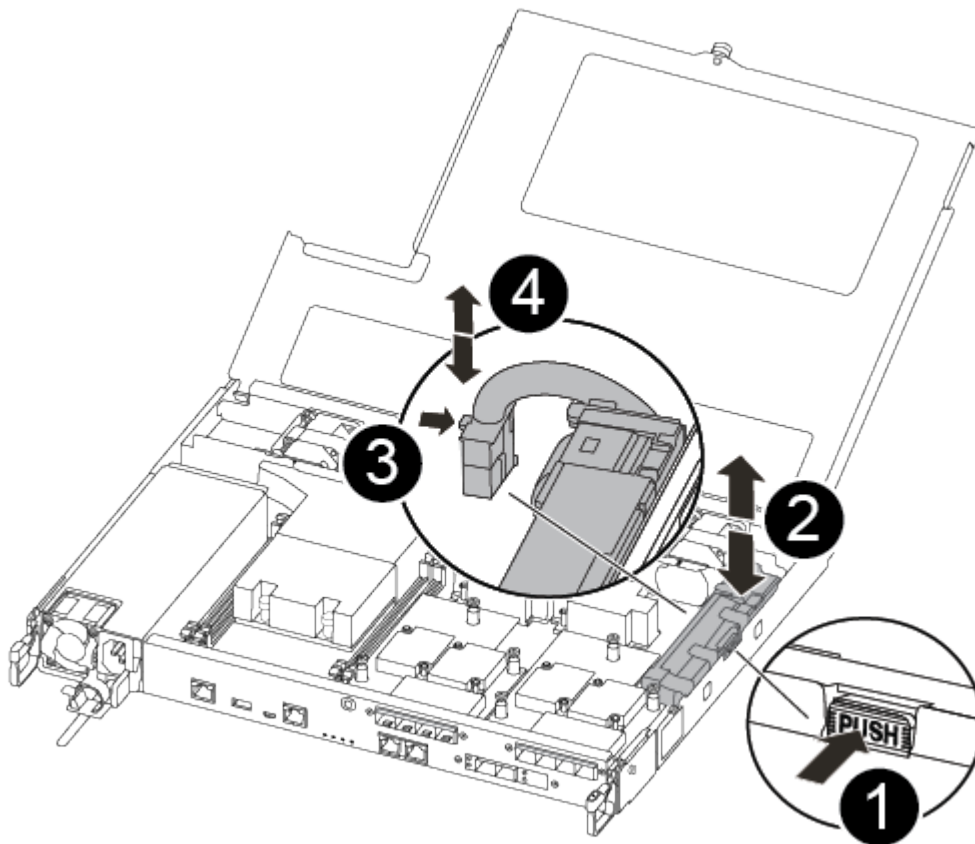
①	Squeeze the clip on the face of the battery plug.
②	Unplug the battery cable from the socket.

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.

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

ℹ️ 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 node where the component is being replaced.

Steps

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. 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.

ℹ️ 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.
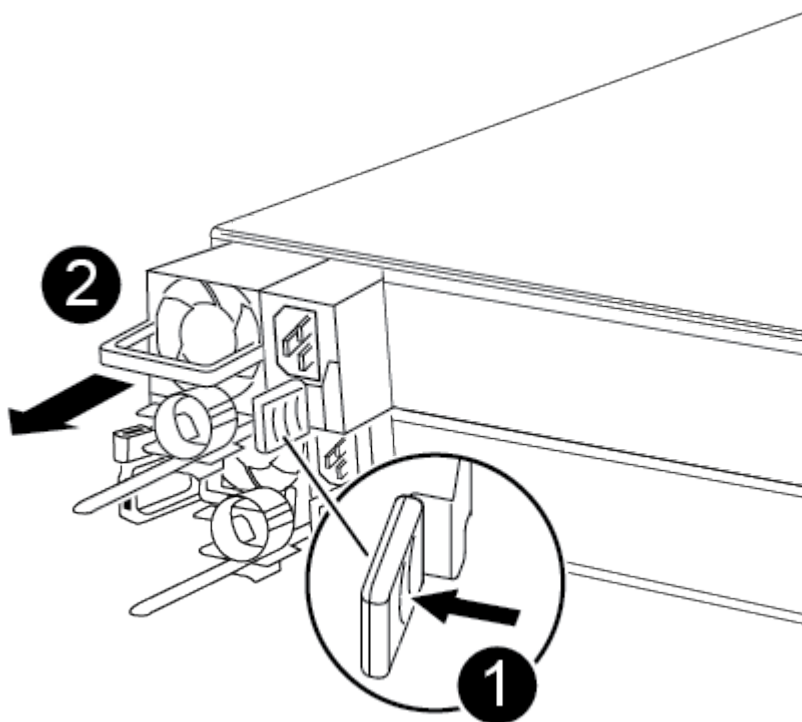
①	Blue power supply locking tab
②	Power supply

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

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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify -node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

If the impaired node 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 node from the healthy node: `storage failover takeover -ofnode impaired_node_name` + When the impaired node 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 node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node 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 node shows false for eligibility and health, you must correct the issue before shutting down the impaired node; 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 node: `storage failover modify –node local -auto-giveback false`

3. Take the impaired node to the LOADER prompt:

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

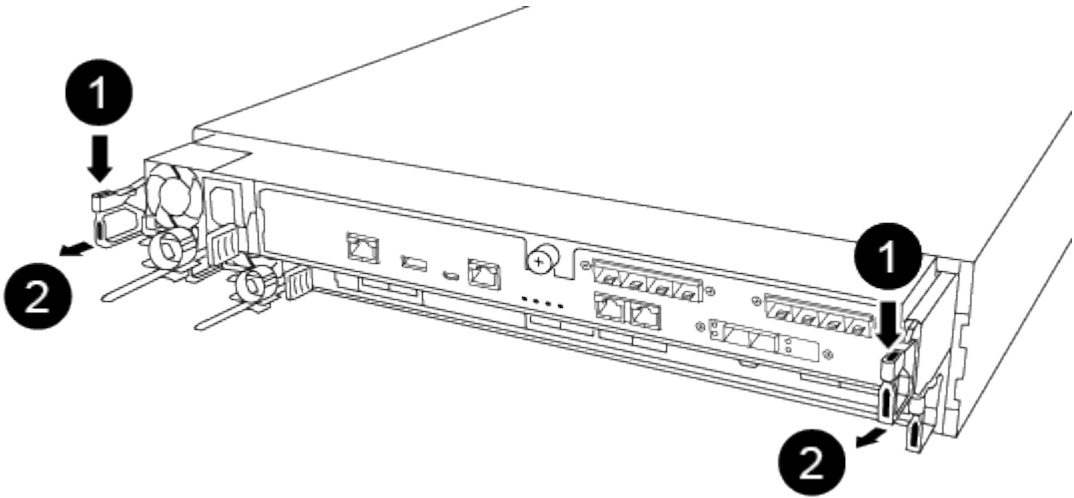## Step 2: Remove the controller module

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.

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

1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.

6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.

❶	Thumbscrew
❷	Controller module cover.

7. Lift out the air duct cover.

Step 3: Replace the RTC battery

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

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

Replacing the RTC battery

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

	Gently pull tab away from the battery housing. NOTE: Pulling it away aggressively might displace the tab.
❷	Lift the battery up. ⓘ Make a note of the polarity of the battery.
❸	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.
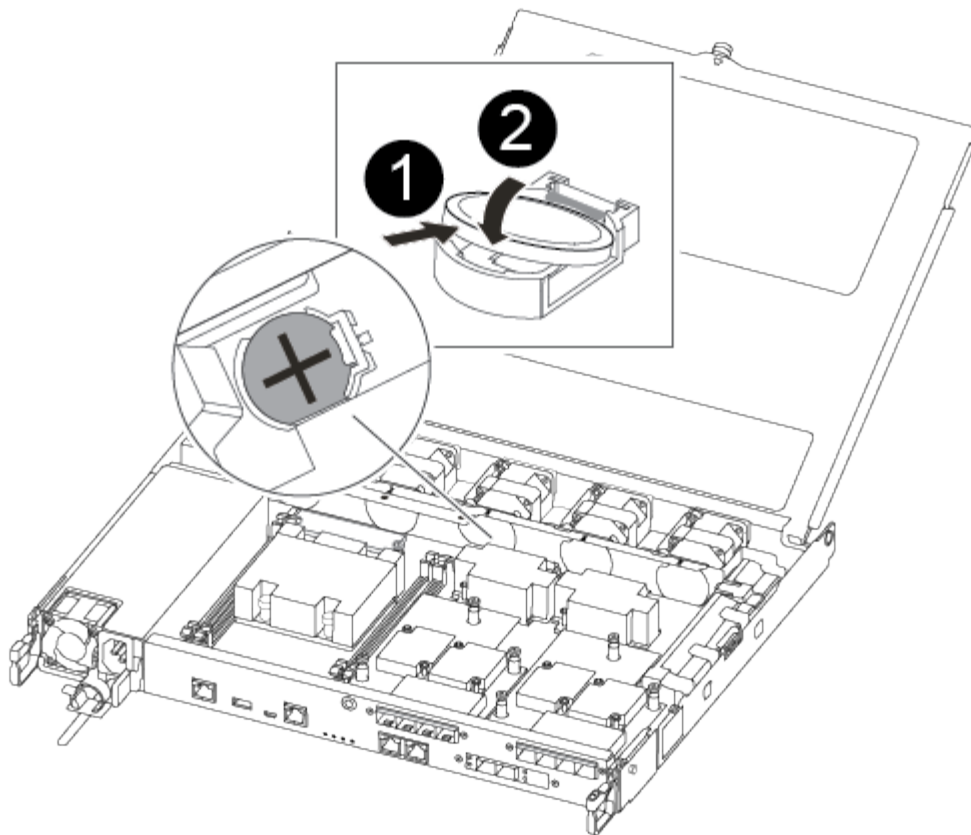
![1]	With positive polarity face up, slide the battery under the tab of the battery housing.
![2]	Push the battery gently into place and make sure the tab secures it to the housing. + **CAUTION:** + Pushing it in aggressively might cause the battery to eject out again.

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 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: 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.