FAS2820 systems

Install and maintain

NetApp
February 06, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems/fas2800/install-setup.html on February 06, 2026. Always check docs.netapp.com for the latest.

Table of Contents

FAS2820 systems

Install and setup

Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

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

- Video steps

  Video step-by-step instructions.

- Detailed steps

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

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

Quick guide - FAS2820

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

Access the *Installation and Setup Instructions* PDF poster:

FAS2820 Systems Installation and Setup Instructions

Video steps - FAS2820

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

Animation - FAS2820 Installation and setup instructions

Detailed steps - FAS2820

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

Step 1: Prepare for installation

Before you begin

You need to provide the following at your site:

- Rack space for the storage system in either a telco rack or system cabinet.
  - 2U for the storage system

- 2U or 4U for each drive shelf in your system
- Phillips #2 screwdriver
- Additional networking cables to connect your storage system to your network switch and laptop or console with a Web browser
- A laptop or console with an RJ-45 connection and access to a Web browser
  - Access to the NetApp Hardware Universe for information about site requirements as well as additional information on your configured storage system.
  - You might also want to have access to the Release Notes for your version of ONTAP 9 for your version of ONTAP for more information about this storage system.

Steps

1. Unpack all boxes and inventory the contents.

   Customers with specific power requirements must check NetApp Hardware Universe for their configuration options.

2. Access the Configure ONTAP on a new cluster with System Manager
   a. Review the requirements amd procedure steps.
   b. Gather information about your storage system by completing the setup worksheet^ (need the URL to the worksheet).
   c. Record the storage system serial number from the controllers.

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

Type of cable…	Part number and length	Connector type	For…
10 GbE, SFP28 cable (order dependent)	X6566B-05-R6, .5, X6566B-2-R6, 2m		Network cable
25Gb Ethernet, SFP28	X66240A-05, .5m X66240-2, 2m X66240A-5, 5m		Network cable
32Gb Fiber Channel, SFP+ (target/initiator)	X66250-2, 2m X66250-5, 5m X66250-15, 15m		FC network

Type of cable…	Part number and length	Connector type	For…
Cat 6, RJ-45 (order dependent)	X6561-R6 X6562-R6		Management network and Ethernet data
Storage	X66030A, 0.5m X66031A, 1m X66032A, 2m		Storage
USB-C console cable	No part number label		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	No part number label		Powering up the storage system
Optional FC cable	Optional FC cable		Additional FC network cable

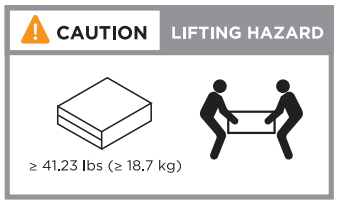
Step 2: Install the hardware

Install your storage system in a telco rack or NetApp storage system cabinet, as applicable.

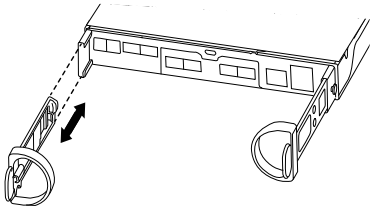
Steps

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

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



3. Attach cable management devices (as shown).



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

Step 3: Cable controllers to your network

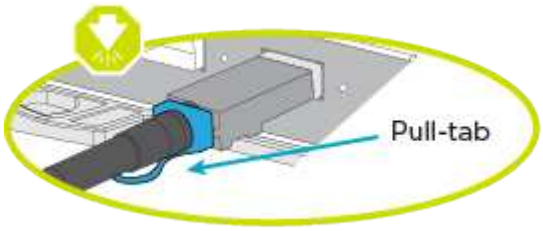
Cable the controllers to your network as either a two-node switchless cluster or a switched cluster.

The following table identifies the cable type with the call out number and cable color in the illustrations for both two-node switchless cluster and switched cluster.

Cabling	Connection type
1	Cluster interconnect
2	Management network switch
3	Host network switches

Before you begin

- Contact your network administrator for information about connecting the storage system to the switches.
- 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 the cable head over and try again.
  - If connecting to an optical switch, insert the SFP into the controller port before cabling to the port.



You can use either the applicable animation or detailed steps in the table to cable your controllers to your network.

Animation - Cabling a two-node switchless cluster cabling

Animation - Switched cluster cabling

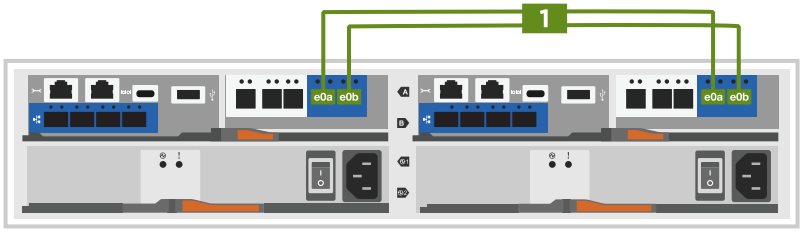
Option 1: Cable a two-node switchless cluster

Cable your network connections and your cluster interconnect ports for a two-node switchless cluster.

Steps

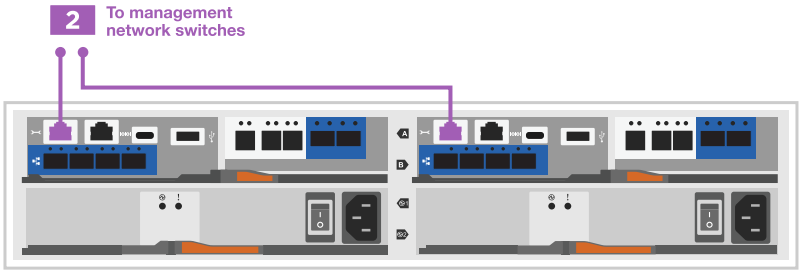
1. Cable the cluster interconnect ports e0a to e0a and e0b to e0b with the cluster interconnect cable:

Cluster interconnect cables

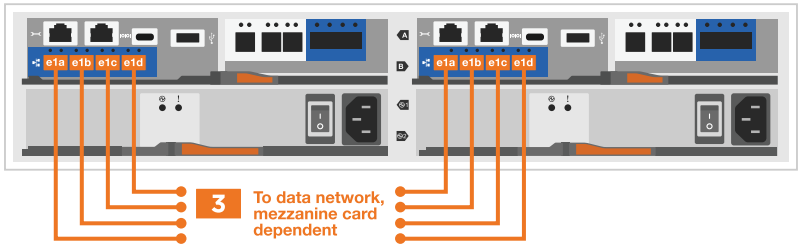


2. Cable the e0M ports to the management network switches with the RJ45 cables:

RJ45 cables

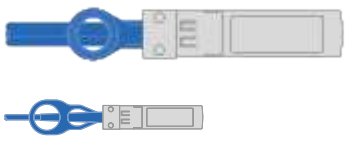


3. Cable the mezzanine card ports to your host network.



   a. If you have a 4-port Ethernet data network, cable ports e1a through e1d to your Ethernet data network.

      - 4-ports, 10/25Gb Ethernet, SFP28



- 4-ports, 10GBASE-T, RJ45

b. If you have a 4-port Fiber Channel data network, cable ports 1a through 1d for your FC network.

- 4-ports, 32Gb Fiber Channel, SFP+ (target only)

- 4-ports, 32Gb Fiber Channel, SFP+ (initiator/target)

c. If you have a 2+2 card (2 ports with Ethernet connections and 2 ports with Fiber Channel connections), cable ports e1a and e1b to your FC data network and ports e1c and e1d to your Ethernet data network.

- 2-ports, 10/25Gb Ethernet (SFP28) + 2-ports 32Gb FC (SFP+)

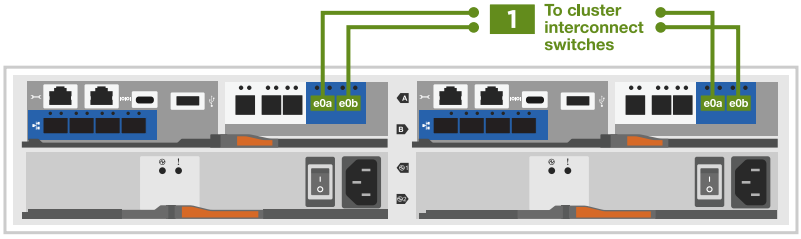
DO NOT plug in the power cords.

Option 2: Cable a switched cluster

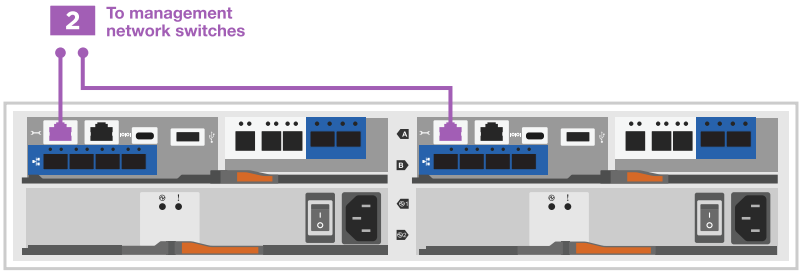
Cable your network connections and your cluster interconnect ports for a switched cluster.

Steps

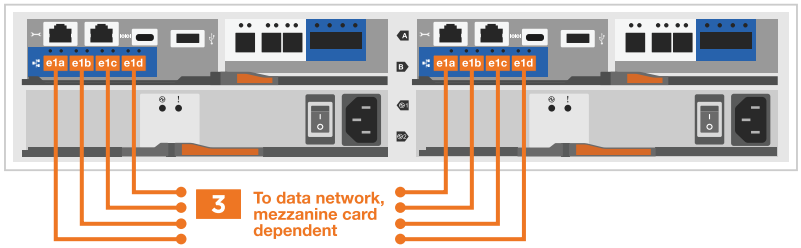
1. Cable the cluster interconnect ports e0a to e0a and e0b to e0b with the cluster interconnect cable:



2. Cable the e0M ports to the management network switches with the RJ45 cables:



3. Cable the mezzanine card ports to your host network.



a. If you have a 4-port Ethernet data network, cable ports e1a through e1d to your Ethernet data network.

   - 4-ports, 10/25Gb Ethernet, SFP28

   - 4-ports, 10GBASE-T, RJ45

b. If you have a 4-port Fiber Channel data network, cable ports 1a through 1d for your FC network.

   - 4-ports, 32Gb Fiber Channel, SFP+ (target only)

   - 4-ports, 32Gb Fiber Channel, SFP+ (initiator/target)

c. If you have a 2+2 card (2 ports with Ethernet connections and 2 ports with Fiber Channel connections), cable ports e1a and e1b to your FC data network and ports e1c and e1d to your Ethernet data network.

   - 2-ports, 10/25Gb Ethernet (SFP28) + 2-ports 32Gb FC (SFP+)

DO NOT plug in the power cords.

Step 4: Cable controllers to drive shelves

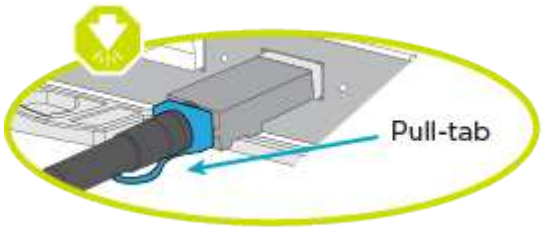
Cable your controllers to external storage.

The following table identifies the cable type with the call out number and cable color in the illustrations for cabling your drive shelves to your storage system.

The example uses DS224C. Cabling is similar with other supported drive shelves. See Install and cable shelves for a new system installation - shelves with IOM12/IOM12B modules for more information.

Cabling	Connection type
1	Shelf-to-shelf cabling
2	Controller A to the drive shelves
3	Controller B to the drive shelves

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



About this task

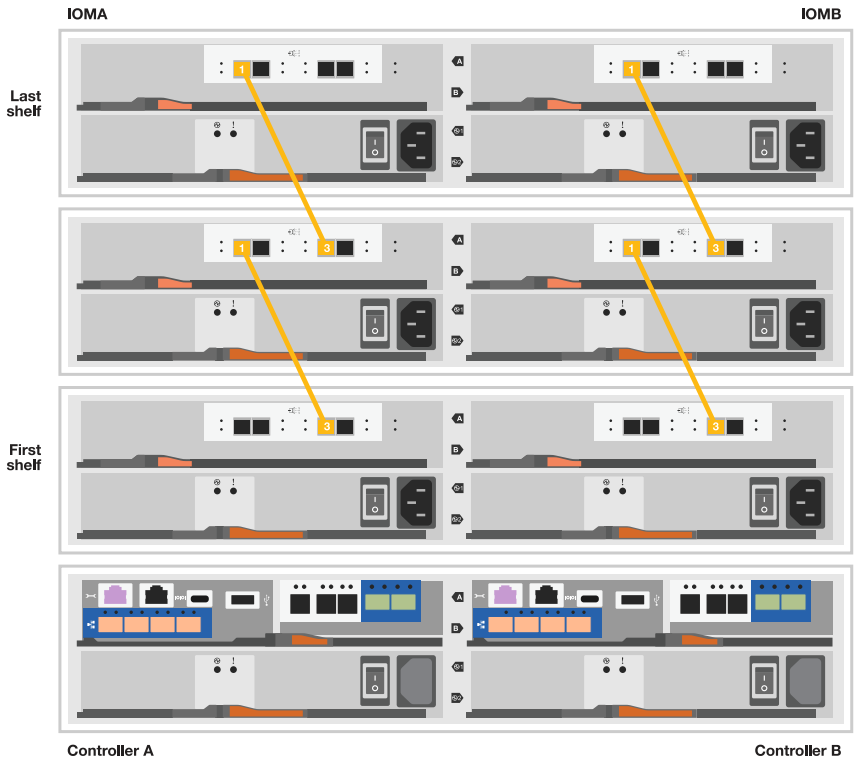
Use the animation or the step-by step instructions to complete the cabling between the controllers and to the drive shelves.

Do not use port 0b2 on a FAS2820. This SAS port is not used by ONTAP and is always disabled. See Install a shelf in a new storage system for more information.

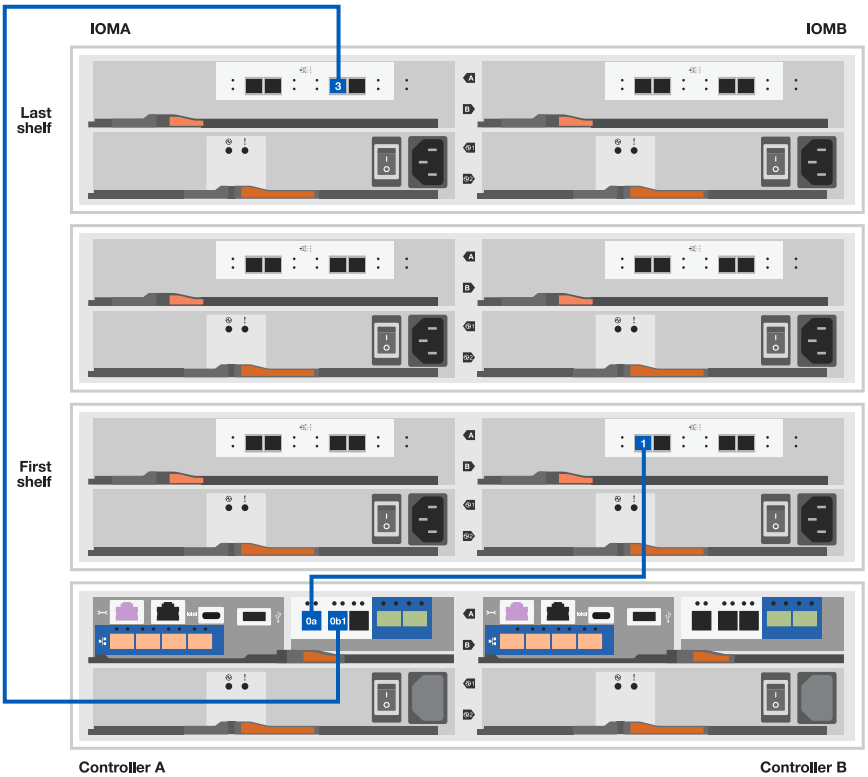
Animation - Drive shelf cabling

Steps

1. Cable the shelf-to-shelf ports.
   a. Port 1 on IOM A to port 3 on the IOM A on the shelf directly below.
   b. Port 1 on IOM B to port 3 on the IOM B on the shelf directly below.



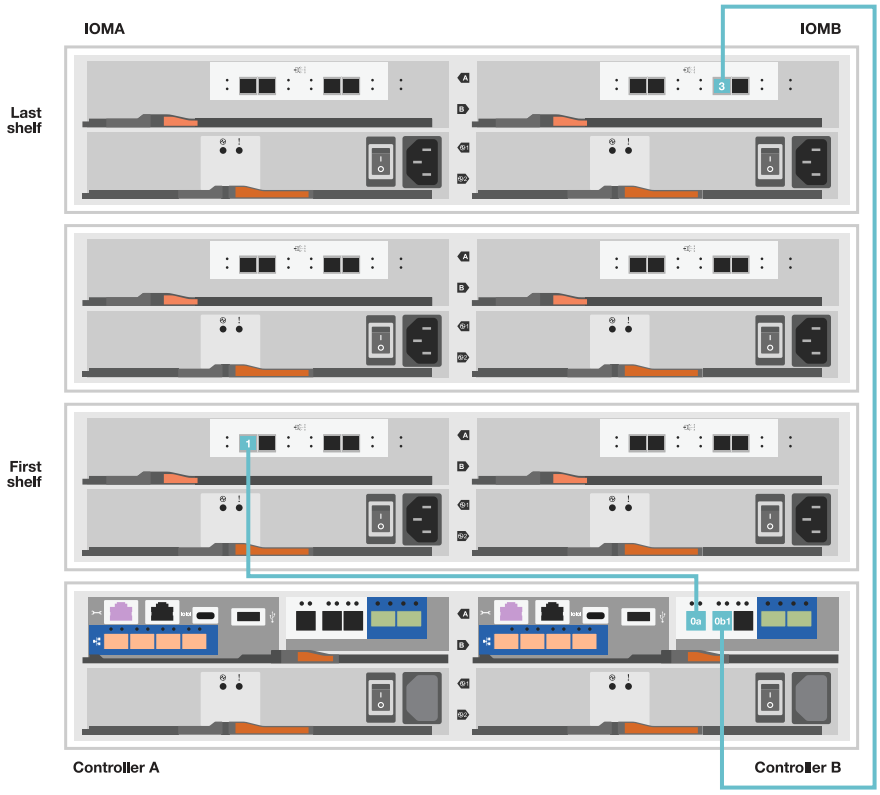
2. Cable controller A to the drive shelves.
   a. Controller A port 0a to IOM B port 1 on first drive shelf in the stack.
   b. Controller A port 0b1 to IOM A port 3 on the last drive shelf in the stack.



3. Connect controller B to the drive shelves.

a. Controller B port 0a to IOM A port 1 on first drive shelf in the stack.

b. Controller B port 0b1 to IOM B port 3 on the last drive shelf in the stack.



Step 5: Complete storage system setup and configuration

Complete your storage system setup and configuration using either Option 1: if network discovery enabled or Option 2: if network discovery is not enabled.

Use the following animation in either option where setting shelf ID is required:

Animation - Set drive shelf IDs

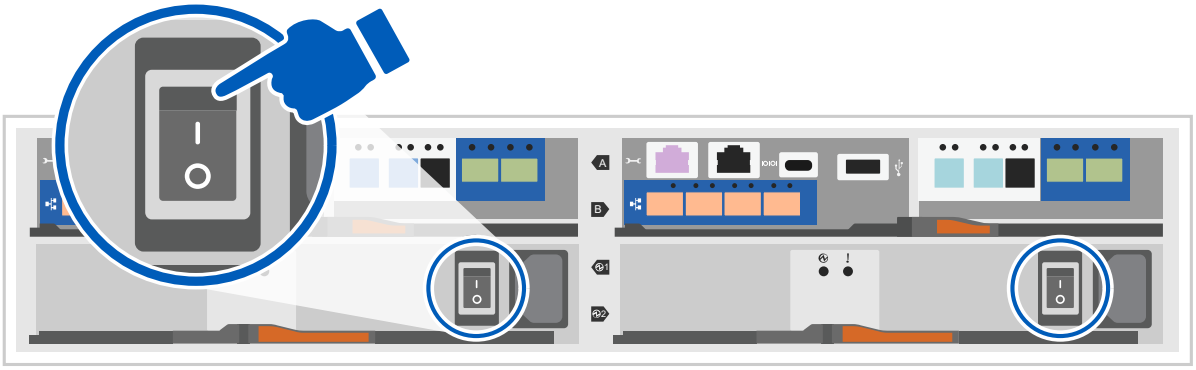
Option 1: If network discovery is enabled

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

Steps

1. Turn on shelf power and set shelf IDsusing the animation at the beginning of this Step.
2. Power on the controllers
   a. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
   b. Turn on the power switches to both nodes.

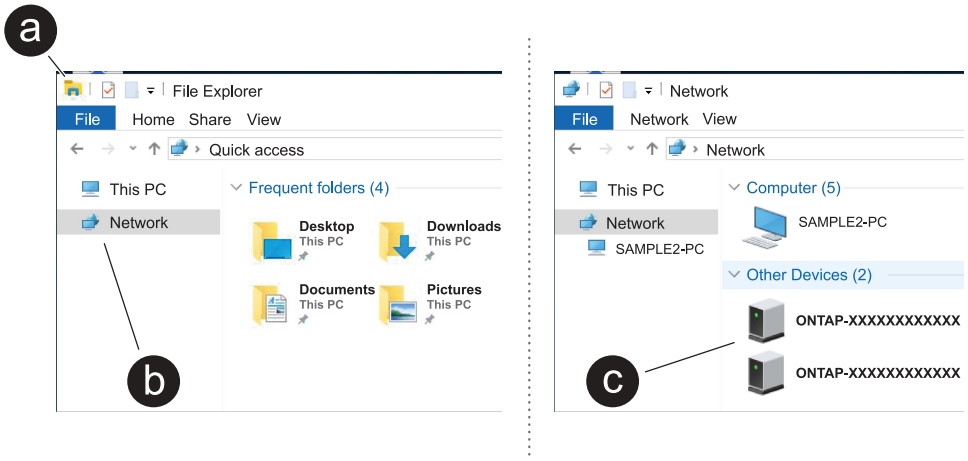
      Initial booting may take up to eight minutes.



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

   See your laptop's online help for more information.

4. Connect your laptop to the Management switch.
5. Use the graphic or steps to discover the storage system node to configure::



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

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

System Manager opens.

6. Use System Manager guided setup to configure your storage system using the data you collected in Step 1: Prepare for installation.
7. Create an account or log into your account.
   a. Click mysupport.netapp.com
   b. Click *Create Account* if you need to create an account or log into your account.
8. Download and install Active IQ Config advisor
   a. Verify the health of your storage system by running Active IQ Config Advisor.
9. Register your system at https://mysupport.netapp.com/site/systems/register.
10. After you have completed the initial configuration, go to the NetApp ONTAP Resources page for information about configuring additional features in ONTAP.

Option 2: If network discovery is not enabled

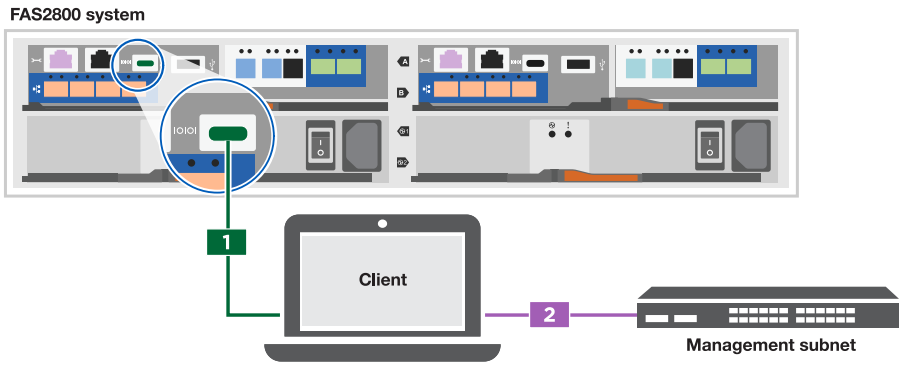
If network discovery is not enabled on your laptop, manually complete the configuration and setup.

Steps

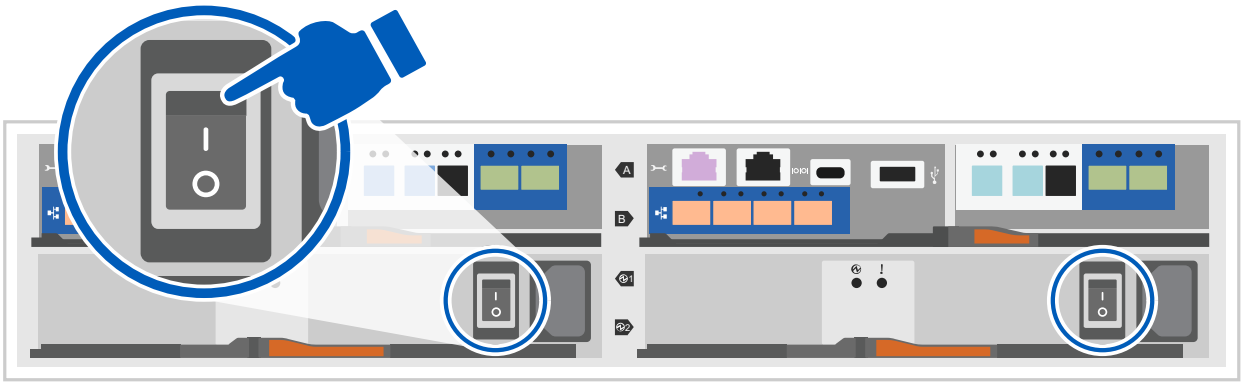
1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

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

   b. Connect the console cable to the laptop or console, and connect the console port on the controller using the console cable that came with your storage system, and then 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. Turn on shelf power and set shelf IDs using the animation at the beginning of this Step.
3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.



Initial booting may take up to eight minutes.

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

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

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.
   The format for the address is https://x.x.x.x.
   b. Configure the storage system using the data you collected in Step 1: Prepare for installation..
7. Create an account or log into your account.
   a. Click mysupport.netapp.com
   b. Click *Create Account* if you need to create an account or log into your account.
8. Download and install Active IQ Config advisor
   a. Verify the health of your storage system by running Active IQ Config Advisor.
9. Register your system at https://mysupport.netapp.com/site/systems/register.
10. After you have completed the initial configuration, go to the NetApp ONTAP Resources page for information about configuring additional features in ONTAP.

Maintain

Maintain FAS2820 hardware

Maintain the hardware of your FAS2820 storage system to ensure long-term reliability and optimal performance. Perform regular maintenance tasks such as replacing faulty components, as this helps prevent downtime and data loss.

The maintenance procedures assume that the FAS2820 storage system has already been deployed as a storage node in the ONTAP environment.

System components

For the FAS2820 storage system, you can perform maintenance procedures on the following components.

Boot media - automated recovery	The boot media stores a primary and secondary set of ONTAP image files that the storage system uses to boot. During automated recovery, the system retrieves the boot image from the partner node and automatically runs the appropriate boot menu option to install the image on your replacement boot media. The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the manual boot recovery procedure.
Boot media - manual recovery	The boot media stores a primary and secondary set of ONTAP image files that the storage system uses to boot. During manual recovery, you boot the storage system from a USB drive and manually restore the file system image and configuration. If your storage system is running ONTAP 9.17.1 and later, use the automated boot recovery procedure.
Caching module	You must replace the controller's caching module when your system registers a single AutoSupport (ASUP) message that the module has gone offline.
Chassis	The chassis is the physical enclosure housing all the controller components such as the controller/CPU unit, power supply, and I/O.
Controller	A controller consists of a board, firmware, and software. It controls the drives and implements the ONTAP functions.
DIMM	You must replace a DIMM (dual in-line memory module) when a memory mismatch is present, or you have a failed DIMM.
Drive	A drive is a device that provides the physical storage media for data.
NVMEM battery	A battery is included with the controller and preserves cached data if the AC power fails.
Mezzanine card	A Mezzanine card is an expansion card that is designed to be inserted into a specialized slot on the motherboard and holds the card I/O cards.

Power supply	A power supply provides a redundant power source in a controller.
Real-time clock battery	A real time clock battery preserves system date and time information if the power is off.

Boot media - automated recovery

Boot media automated recovery workflow - FAS2800

The automated recovery of the boot image involves the system automatically identifying and selecting the appropriate boot menu option. It uses the boot image on partner node to reinstall ONTAP on the replacement boot media in your FAS2800 storage system.

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

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

1. **Review the boot media requirements**

Review the requirements for boot media replacement.

2. **Shut down the controller**

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

3. **Replace the boot media**

Remove the failed boot media from the System Management module and install the replacement boot media.

4. **Restore the image on the boot media**

Restore the ONTAP image from the partner controller.

5. **Return the failed part to NetApp**

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

Requirements for automated boot media recovery - FAS2800

Before replacing the boot media in your FAS2800 system, ensure you meet the necessary requirements for a successful replacement. This includes verifying that you have the correct replacement boot media, confirming that the e0S (e0M wrench) port on the impaired controller is not faulty, and determining whether Onboard Key Manager (OKM) or External Key Manager (EKM) is enabled.

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

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

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

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

What's next

After you've reviewed the boot media requirements, you shut down the controller.

Shut down the controller for automated boot media recovery - FAS2800

Shut down the impaired controller in your FAS2800 storage system to prevent data loss and maintain system stability during the automated boot media recovery process.

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

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

About this task

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

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

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

Steps

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

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

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

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

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

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

   b. Enter `y` when you see the prompt *Do you want to disable auto-giveback?*
3. Take the impaired controller to the LOADER prompt:

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

What's next

After you shut down the impaired controller, you replace the boot media.

Replace the boot media for automated boot recovery - FAS2800

The boot media in your FAS2800 system stores essential firmware and configuration data. The replacement process involves removing and opening the controller module, removing the impaired boot media, installing the replacement boot media in the controller module, and then reinstalling the controller module.

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

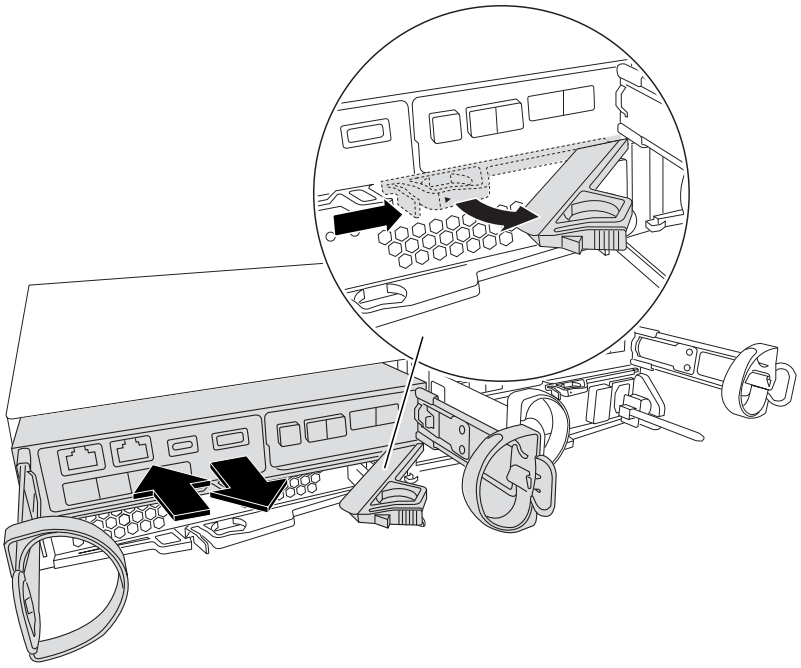
The boot media is located inside the controller module and is accessed by removing the controller module from the chassis and removing the controller module cover.module from the system.

Steps

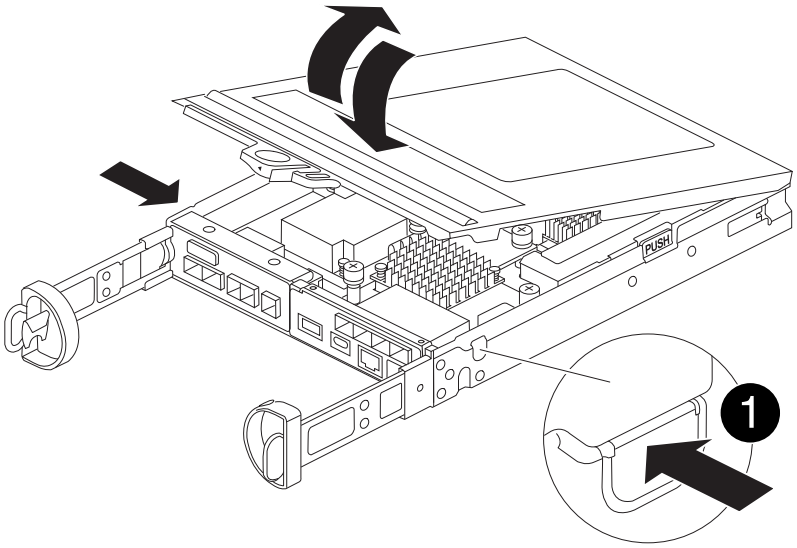
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the

system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

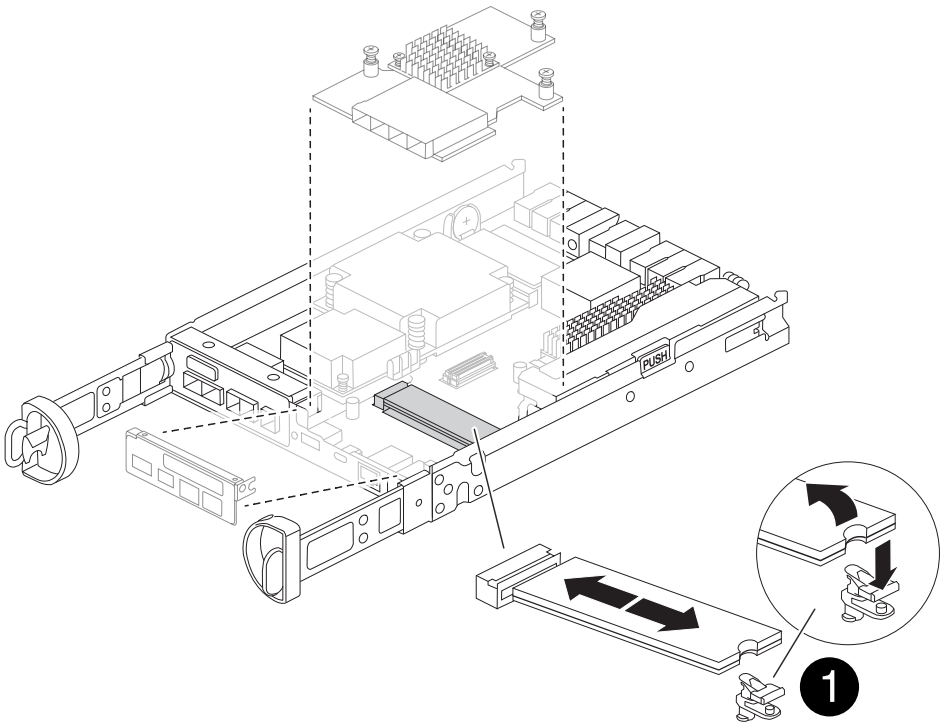


4. Turn the controller module over and place it on a flat, stable surface.
5. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



1	Controller module cover release button

6. Locate the boot media in the controller module, located under the mezzanine card and follow the directions to replace it.



1	Boot media locking tab

7. Remove the mezzanine card using the following illustration or the FRU map on the controller module:
   a. Remove the IO Plate by sliding it straight out from thr controller module.
   b. Loosen the thumbscrews on the mezzanine card.

      You can loosen the thumbscrews with your fingers or a screwdriver. If you use your fingers, you might need to rotate the NV battery up for better finger purchase on the thumbscrew next to it.

   c. Lift the mezzanine card straight up.
8. Replace the boot media:
   a. Press the blue button on the boot media housing to release the boot media from its housing, rotate the boot media up, and then gently pull it straight out of the boot media socket.

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

   b. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket. Check the boot media to make sure that it is seated squarely and completely in the socket, and if necessary, remove the boot media and reseat it into the socket.
   c. Push the blue locking button, rotate the boot media all the way down, and then release the locking button to lock the boot media in place.
9. Reinstall the mezzanine card:
   a. Align the socket on the motherboard with the socket on the mezzanine card, and then gently seat the card in the socket.

b. Tighten the three thumbscrews on the mezzanine card.

c. Reinstall the IO Plate.

10. Reinstall the controller module cover and lock it into place.

11. Install the controller module:

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

    b. Recable the controller, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

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

What's next

After physically replacing the impaired boot media, restore the ONTAP image from the partner node.

Automated boot media recovery from the partner node - FAS2800

After installing the new boot media device in your FAS2800 system, you can start the automated boot media recovery process to restore the configuration from the partner node. During the recovery process, the system checks whether encryption is enabled and determines the type of key encryption in use. If key encryption is enabled, the system guides you through the appropriate steps to restore it.

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

Before you begin

- Determine your key manager type:
  - Onboard Key Manager (OKM): Requires cluster-wide passphrase and backup data
  - External Key Manager (EKM): Requires the following files from the partner node:
    - `/cfcard/kmip/servers.cfg`
    - `/cfcard/kmip/certs/client.crt`
    - `/cfcard/kmip/certs/client.key`
    - `/cfcard/kmip/certs/CA.pem`

Steps

1. From the LOADER prompt, start the boot media recovery process:

   ```
   boot_recovery -partner
   ```

   The screen displays the following message:

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

2. Monitor the boot media install recovery process.

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

3. The system checks for encryption and displays one of the following messages:

If you see this message…	Do this…
`key manager is not configured. Exiting.`	Encryption is not installed on the system. a. Wait for the login prompt to display. b. Log into the node and give back the storage: `storage failover giveback -ofnode` *`impaired_node_name`* c. Go to re-enabling automatic giveback if it was disabled.
`key manager is configured.`	Encryption is installed. Go to restoring the key manager.

> If the system cannot identify the key manager configuration, it displays an error message and prompts you to confirm whether key manager is configured and which type (onboard or external). Answer the prompts to proceed.

4. Restore the key manager using the appropriate procedure for your configuration:

Onboard Key Manager (OKM)

The system displays the following message and begins running BootMenu Option 10:

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

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

a. Enter `y` at the prompt to confirm you want to start the OKM recovery process.

b. Enter the passphrase for onboard key management when prompted.

c. Enter the passphrase again when prompted to confirm.

d. Enter the backup data for onboard key manager when prompted.

Show example of passphrase and backup data prompts

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

e. Monitor the recovery process as it restores the appropriate files from the partner node.

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

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

Successfully recovered keymanager secrets.
```

f. After the node reboots, verify that the system is back online and operational.

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

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

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

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

Go to re-enabling automatic giveback if it was disabled.

External Key Manager (EKM)

The system displays the following message and begins running BootMenu Option 11:

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

a. Enter the EKM configuration settings when prompted:

i. Enter the client certificate contents from the `/cfcard/kmip/certs/client.crt` file:

Show example of client certificate contents

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

ii. Enter the client key file contents from the `/cfcard/kmip/certs/client.key` file:

Show example of client key file contents

```
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
```

iii. Enter the KMIP server CA(s) file contents from the `/cfcard/kmip/certs/CA.pem` file:

Show example of KMIP server file contents

```
-----BEGIN CERTIFICATE-----
<KMIP_certificate_CA_value>
-----END CERTIFICATE-----
```

iv. Enter the server configuration file contents from the `/cfcard/kmip/servers.cfg` file:

Show example of server configuration file contents

```
xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx:5696.port=5696
xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4
1xxx.xxx.xxx.xxx:5696.timeout=25
xxx.xxx.xxx.xxx:5696.nbio=1
xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.cr
t
xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:
!RC2:!RC4:!SEED:!eNULL:!aNULL"
xxx.xxx.xxx.xxx:5696.verify=true
xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>
```

v. If prompted, enter the ONTAP Cluster UUID from the partner node. You can check the cluster UUID from the partner node using the `cluster identify show` command.

Show example of ONTAP Cluster UUID prompt

```
Notice: bootarg.mgwd.cluster_uuid is not set or is empty.
Do you know the ONTAP Cluster UUID? {y/n} y
Enter the ONTAP Cluster UUID: <cluster_uuid_value>


System is ready to utilize external key manager(s).
```

vi. If prompted, enter the temporary network interface and settings for the node:

- The IP address for the port
- The netmask for the port
- The IP address of the default gateway

Show example of temporary network setting prompts

```
In order to recover key information, a temporary network
interface needs to be
configured.

Select the network port you want to use (for example,
'e0a')
e0M

Enter the IP address for port : xxx.xxx.xxx.xxx
Enter the netmask for port : xxx.xxx.xxx.xxx
Enter IP address of default gateway: xxx.xxx.xxx.xxx
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
```

b. Verify the key restoration status:

- If you see `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` in the output, the EKM configuration has been successfully restored. The process restores the appropriate files from the partner node and reboots the node. Proceed to the next step.
- If the key is not successfully restored, the system halts and displays error and warning messages. Rerun the recovery process from the LOADER prompt: `boot_recovery -partner`

Show example of key recovery error and warning messages

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

Uptime: 11m32s
System halting...

LOADER-B>
```

c. After the node reboots, verify that the system is back online and operational.

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

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

Go to re-enabling automatic giveback if it was disabled.

5. If automatic giveback was disabled, reenable it:

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

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

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

What's next

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

Return the failed boot media to NetApp - FAS2800

If a component in your FAS2800 system fails, return the failed part to NetApp. See the Part Return and Replacements page for further information.

Boot Media - manual recovery

Boot media manual recovery workflow - FAS2800

Get started with replacing the boot media in your FAS2800 storage system by reviewing the replacement requirements, checking encryption status, shutting down the controller, replacing the boot media, booting the recovery image, restoring encryption, and verifying the system functionality.

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

Review the boot media requirements

Review the requirements for replacing the boot media.

Check encryption key support and status

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

Shut down the controller

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

Replace the boot media

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

Boot the recovery image

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

Restore encryption

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

Return the failed part to NetApp

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

Requirements for manual boot media recovery - AFF A800

Before replacing the boot media in your AFF A800 system, ensure you meet the necessary requirements for a successful replacement. This includes making sure you have a USB flash drive with the appropriate amount of storage and verifying that you

have the correct replacement boot device.

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

USB flash drive

- Ensure you have a USB flash drive formatted to FAT32.
- The USB must have sufficient storage capacity to hold the `image_xxx.tgz` file.

File preparation

Copy the `image_xxx.tgz` file to the USB flash drive. This file will be used when you transfer the ONTAP image using the USB flash drive.

Component replacement

Replace the failed component with the replacement component provided by NetApp.

Controller identification

It is critical to apply the commands to the correct controller when you are replacing the impaired boot media:

- The *impaired controller* is the controller on which you are performing maintenance.
- The *healthy controller* is the HA partner of the impaired controller.

What's next?

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

Check encryption key support and status - FAS2820

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

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

Step 1: Check NVE support and download the correct ONTAP image

Determine whether your ONTAP version supports NetApp Volume Encryption (NVE) so you can download the correct ONTAP image for the boot media replacement.

Steps

1. Check if your ONTAP version supports encryption:

   ```
   version -v
   ```

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

2. Download the appropriate ONTAP image based on NVE support:
   - If NVE is supported: Download the ONTAP image with NetApp Volume Encryption

- If NVE is not supported: Download the ONTAP image without NetApp Volume Encryption

> Download the ONTAP image from the NetApp Support Site to your HTTP or FTP server or a local folder. You will need this image file during the boot media replacement procedure.

Step 2: Verify key manager status and back up configuration

Before shutting down the impaired controller, verify the key manager configuration and back up the necessary information.

Steps

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

ONTAP version	Run this command
ONTAP 9.14.1 or later	`security key-manager keystore show` • If EKM is enabled, `EKM` is listed in the command output. • If OKM is enabled, `OKM` is listed in the command output. • If no key manager is enabled, `No key manager keystores configured` is listed in the command output.
ONTAP 9.13.1 or earlier	`security key-manager show-key-store` • If EKM is enabled, `external` is listed in the command output. • If OKM is enabled, `onboard` is listed in the command output. • If no key manager is enabled, `No key managers configured` is listed in the command output.

2. Depending on whether a key manager is configured on your system, do one of the following:

   If no key manager is configured:

   You can safely shut down the impaired controller and proceed to the shutdown procedure.

   If a key manager is configured (EKM or OKM):

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

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

   b. Review the output and check the value in the `Restored` column. This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Complete the appropriate procedure based on your key manager type:

External Key Manager (EKM)

Complete these steps based on the value in the `Restored` column.

If all keys show `true` in the Restored column:

You can safely shut down the impaired controller and proceed to the shutdown procedure.

If any keys show a value other than `true` in the Restored column:

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.

b. Verify that all authentication keys are restored:

   `security key-manager key query`

   Confirm that the `Restored` column displays `true` for all authentication keys.

c. If all keys are restored, you can safely shut down the impaired controller and proceed to the shutdown procedure.

Onboard Key Manager (OKM)

Complete these steps based on the value in the `Restored` column.

If all keys show `true` in the Restored column:

a. Back up the OKM information:
   i. Switch to advanced privilege mode:

      `set -priv advanced`

      Enter `y` when prompted to continue.

   ii. Display the key management backup information:

      `security key-manager onboard show-backup`

   iii. Copy the backup information to a separate file or your log file.

      You will need this backup information if you need to manually recover OKM during the replacement procedure.

   iv. Return to admin mode:

      `set -priv admin`

b. You can safely shut down the impaired controller and proceed to the shutdown procedure.

If any keys show a value other than `true` in the Restored column:

a. Synchronize the onboard key manager:

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

Enter the 32-character alphanumeric onboard key management passphrase when prompted.

> This is the cluster-wide passphrase you created when you initially configured the Onboard Key Manager. If you do not have this passphrase, contact NetApp Support.

b. Verify all authentication keys are restored:

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

Confirm that the `Restored` column displays `true` for all authentication keys and the `Key Manager` type shows `onboard`.

c. Back up the OKM information:

i. Switch to advanced privilege mode:

```
set -priv advanced
```

Enter `y` when prompted to continue.

ii. Display the key management backup information:

```
security key-manager onboard show-backup
```

iii. Copy the backup information to a separate file or your log file.

You will need this backup information if you need to manually recover OKM during the replacement procedure.

iv. Return to admin mode:

```
set -priv admin
```

d. You can safely shut down the impaired controller and proceed to the shutdown procedure.

What's next?

After checking the encryption key support and status on the boot media, you need to shut down the controller.

Shut down the controller for manual boot media recovery - FAS2820

Shut down or take over the impaired controller.

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

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

What's next?

After shutting down the controller, you need to replace the boot media.

Replace the boot media and prepare for manual boot recovery - FAS2820

You must remove and open the impaired controller module, locate and replace the boot media in the controller, transfer the boot image to a USB drive, insert the USB drive in the controller, and then boot the controller.

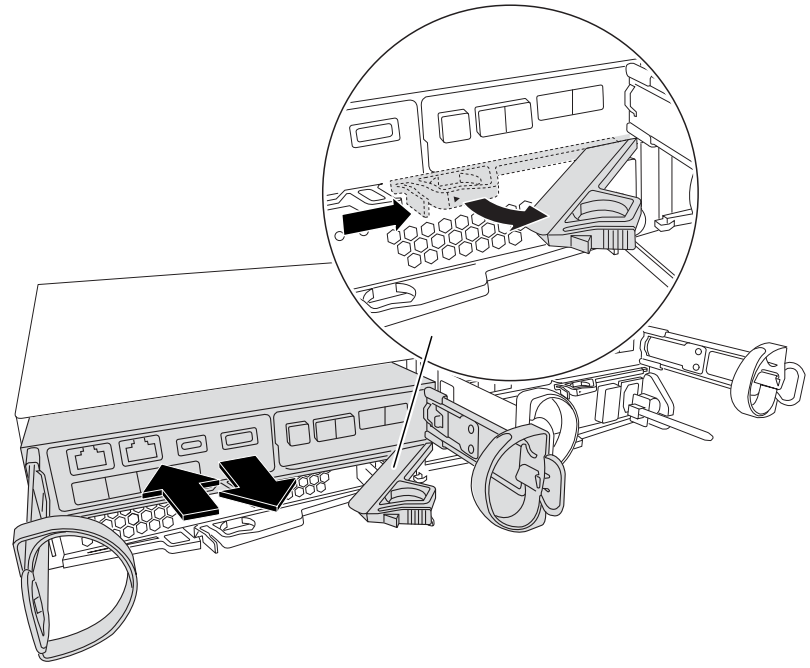
If your storage system is running ONTAP 9.17.1 or later, use the automated boot recovery procedure. If your system is running an earlier version of ONTAP, you must use the manual boot recovery procedure.

Step 1: Remove the controller module

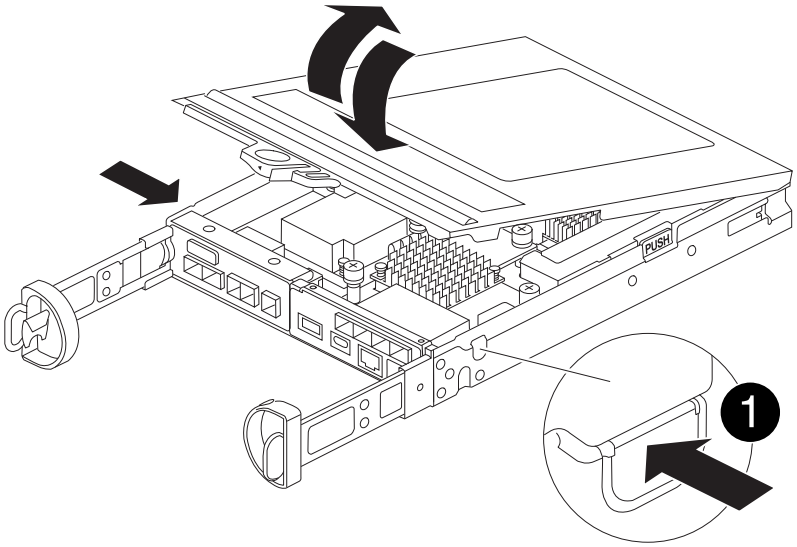
Steps

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

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.
3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



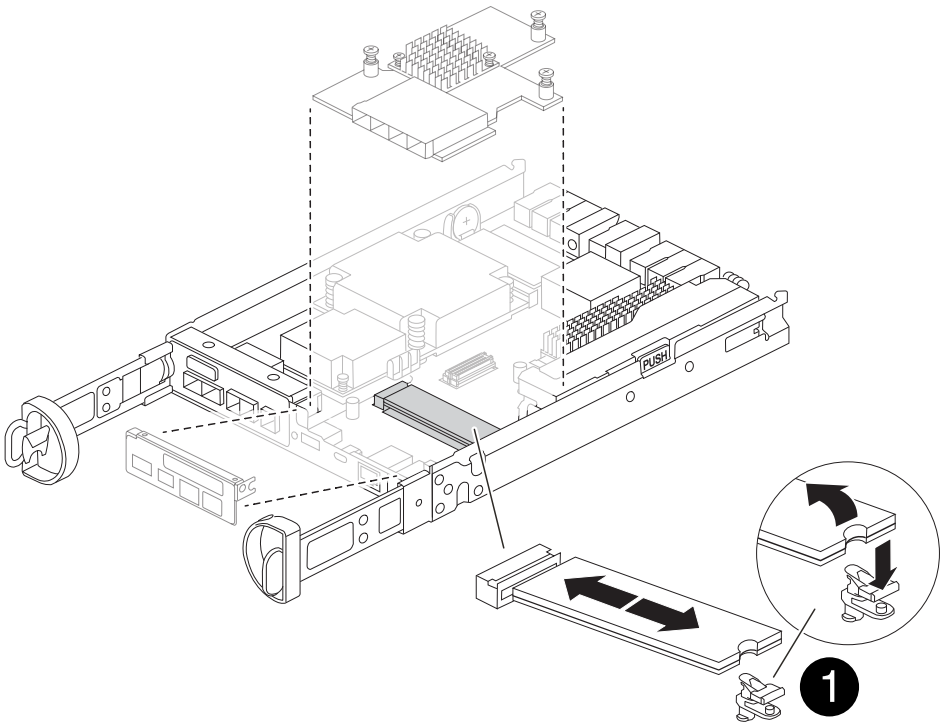
4. Turn the controller module over and place it on a flat, stable surface.
5. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



1	Controller module cover release button

Step 2: Replace the boot media

Locate the boot media in the controller module, located under the mezzanine card and follow the directions to replace it.



1	Boot media locking tab

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the mezzanine card using the following illustration or the FRU map on the controller module:
   a. Remove the IO Plate by sliding it straight out from thr controller module.
   b. Loosen the thumbscrews on the mezzanine card.

      You can loosen the thumbscrews with your fingers or a screwdriver. If you use your fingers, you might need to rotate the NV battery up for better finger purchase on the thumbscrew next to it.

   c. Lift the mezzanine card straight up.
3. Replace the boot media:
   a. Press the blue button on the boot media housing to release the boot media from its housing, rotate the boot media up, and then gently pull it straight out of the boot media socket.

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

   b. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket. Check the boot media to make sure that it is seated squarely and completely in the socket, and if necessary, remove the boot media and reseat it into the socket.
   c. Push the blue locking button, rotate the boot media all the way down, and then release the locking button to lock the boot media in place.
4. Reinstall the mezzanine card:

a. Align the socket on the motherboard with the socket on the mezzanine card, and then gently seat the card in the socket.

b. Tighten the three thumbscrews on the mezzanine card.

c. Reinstall the IO Plate.

5. Reinstall the controller module cover and lock it into place.

Step 3: Transfer the boot image to the boot media

Install the system image on the replacement boot media using a USB flash drive with the image installed on it. You must restore the var file system during this procedure.

Before you begin

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity.
- You must have a network connection.

Steps

1. Download the appropriate image version of ONTAP to the formatted USB flash drive:

   a. Use How to determine if the running ONTAP version supports NetApp Volume Encryption (NVE) to determine if volume encryption is currently supported.

      - If NVE is supported on the cluster, download the image with NetApp Volume Encryption.
      - If NVE is not supported on the cluster, download the image without NetApp Volume Encryption. See Which ONTAP image should I download? With or without Volume Encryption? for more details.

2. Remove the USB flash drive from your laptop.

3. Install the controller module:

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

   b. Recable the controller module.

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

4. 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.

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

   The controller begins to boot as soon as it is completely installed into the chassis and stops at the LOADER prompt.

What's next?

After replacing the boot media, you need to boot the recovery image.

Manual boot media recovery from a USB drive - FAS2820

After installing the new boot media device in your system, you can boot the recovery

image from a USB drive and restore the configuration from the partner node.

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

Before you begin

- Ensure your console is connected to the impaired controller.
- Verify you have a USB flash drive with the recovery image.
- Determine if your system uses encryption. You will need to select the appropriate option in step 3 based on whether encryption is enabled.

Steps

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

   ```
   boot_recovery
   ```

   The recovery image is downloaded from the USB flash drive.

2. When prompted, enter the name of the image or press **Enter** to accept the default image displayed in brackets.
3. Restore the var file system using the procedure for your ONTAP version:

ONTAP 9.16.0 or earlier

Complete the following steps on the impaired controller and partner controller:

a. **On the impaired controller:** Press `Y` when you see `Do you want to restore the backup configuration now?`

b. **On the impaired controller:** If prompted, press `Y` to overwrite */etc/ssh/ssh_host_ecdsa_key*.

c. **On the partner controller:** Set the impaired controller to advanced privilege level:

```
set -privilege advanced
```

d. **On the partner controller:** Run the restore backup command:

```
system node restore-backup -node local -target-address impaired_node_IP_address
```

> If you see any message other than a successful restore, contact NetApp Support.

e. **On the partner controller:** Return to admin level:

```
set -privilege admin
```

f. **On the impaired controller:** Press `Y` when you see `Was the restore backup procedure successful?`

g. **On the impaired controller:** Press `Y` when you see `...would you like to use this restored copy now?`

h. **On the impaired controller:** Press `Y` when prompted to reboot, then press `Ctrl-C` when you see the Boot Menu.

i. **On the impaired controller:** Do one of the following:

- If the system does not use encryption, select *Option 1 Normal Boot* from the Boot Menu.
- If the system uses encryption, go to Restore encryption.

ONTAP 9.16.1 or later

Complete the following steps on the impaired controller:

a. Press `Y` when prompted to restore the backup configuration.

   After the restore procedure is successful, this message displays: `syncflash_partner: Restore from partner complete`

b. Press `Y` when prompted to confirm that the restore backup was successful.

c. Press `Y` when prompted to use the restored configuration.

d. Press `Y` when prompted to reboot the node.

e. Press `Y` when prompted to reboot again, then press `Ctrl-C` when you see the Boot Menu.

f. Do one of the following:

- If the system does not use encryption, select *Option 1 Normal Boot* from the Boot Menu.

- If the system uses encryption, go to Restore encryption.

4. Connect the console cable to the partner controller.
5. Return the controller to normal operation by giving back its storage:

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

6. If you disabled automatic giveback, reenable it:

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

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

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

What's next?

After booting the recovery image, you need to restore encryption on the boot media.

Restore encryption - FAS2820

Restore encryption on the replacement boot media.

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

Complete the appropriate steps to restore encryption on your system based on your key manager type. If you are unsure which key manager your system uses, check the settings you captured at the beginning of the boot media replacement procedure.

Onboard Key Manager (OKM)

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

Before you begin

Ensure you have the following information available:

- Cluster-wide passphrase entered while enabling onboard key management
- Backup information for the Onboard Key Manager
- Verification that you have the correct passphrase and backup data using the How to verify onboard key management backup and cluster-wide passphrase procedure

Steps

On the impaired controller:

1. Connect the console cable to the impaired controller.
2. From the ONTAP boot menu, select the appropriate option:

ONTAP version	Select this option
ONTAP 9.8 or later	Select option 10. **Show example boot menu** Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10

ONTAP version	Select this option

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

3. Confirm that you want to continue the recovery process when prompted:

   Show example prompt

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

4. Enter the cluster-wide passphrase twice.

   While entering the passphrase, the console does not show any input.

   Show example prompt

   ```
   Enter the passphrase for onboard key management:

   Enter the passphrase again to confirm:
   ```

5. Enter the backup information:

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

Show example prompt

```
Enter the backup data:

---------------------------BEGIN
BACKUP---------------------------
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
34567890123456789012345678901234567890123456789012345678901234
56
45678901234567890123456789012345678901234567890123456789012345
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA

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

b. Press Enter twice at the end of the input.

   The recovery process completes and displays the following message:

   ```
   Successfully recovered keymanager secrets.
   ```

Show example prompt

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

Successfully recovered keymanager secrets.

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

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

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

Show example prompt

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


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

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

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

   On the partner controller:

8. Giveback the impaired controller:

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

   On the impaired controller:

9. After booting with only the CFO aggregate, synchronize the key manager:

   `security key-manager onboard sync`

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

Show example prompt

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

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

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

11. Verify that all keys are synced:

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

    The command should return no results. If any results appear, repeat the sync command until no results are returned.

    On the partner controller:

12. Giveback the impaired controller:

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

13. Restore automatic giveback if you disabled it:

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

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

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

External Key Manager (EKM)

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

Before you begin

Gather the following files from another cluster node or from your backup:

- `/cfcard/kmip/servers.cfg` file or the KMIP server address and port
- `/cfcard/kmip/certs/client.crt` file (client certificate)
- `/cfcard/kmip/certs/client.key` file (client key)
- `/cfcard/kmip/certs/CA.pem` file (KMIP server CA certificates)

Steps

On the impaired controller:

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

   Show example boot menu

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

3. Confirm you have gathered the required information when prompted:

   Show example prompt

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

4. Enter the client and server information when prompted:
   a. Enter the client certificate (client.crt) file contents, including the BEGIN and END lines.
   b. Enter the client key (client.key) file contents, including the BEGIN and END lines.
   c. Enter the KMIP server CA(s) (CA.pem) file contents, including the BEGIN and END lines.
   d. Enter the KMIP server IP address.
   e. Enter the KMIP server port (press Enter to use the default port 5696).

Show example

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

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

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

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

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

The recovery process completes and displays the following message:

```
Successfully recovered keymanager secrets.
```

Show example

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

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

Show example prompt

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

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

6. Restore automatic giveback if you disabled it:

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

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

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

What's next?

After restoring encryption on the boot media, you need to return the failed part to NetApp.

Return the failed boot media to NetApp - FAS2820

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

Replace the caching module - FAS2820

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

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

Step 1: Shut down the impaired controller

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

About this task

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

ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

Steps

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run -node node name localhost -device-id device_number`

      Run the `system controller flash-cache show` command if you don't know the Flash Cache device ID.

   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show`

      The output should display the caching module status as erased.

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

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

3. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
4. Take the impaired controller to the LOADER prompt:

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

If the impaired controller is displaying…	Then…
System prompt or password prompt (enter system password)	Take over or halt the impaired controller: • For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. • For a stand-alone system: `system node halt impaired_node_name`

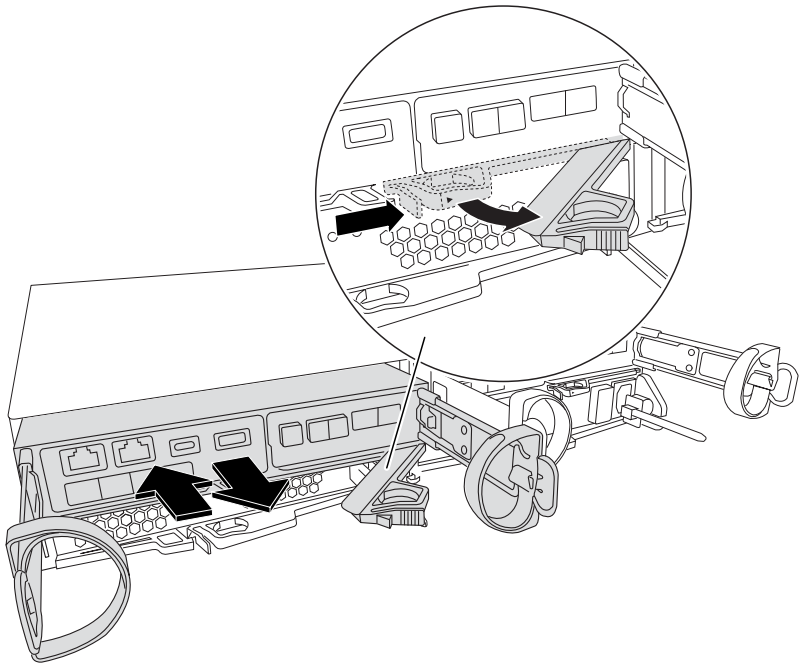
Step 2: Remove controller module

Remove the controller module from the system and then remove the cover on the controller module.

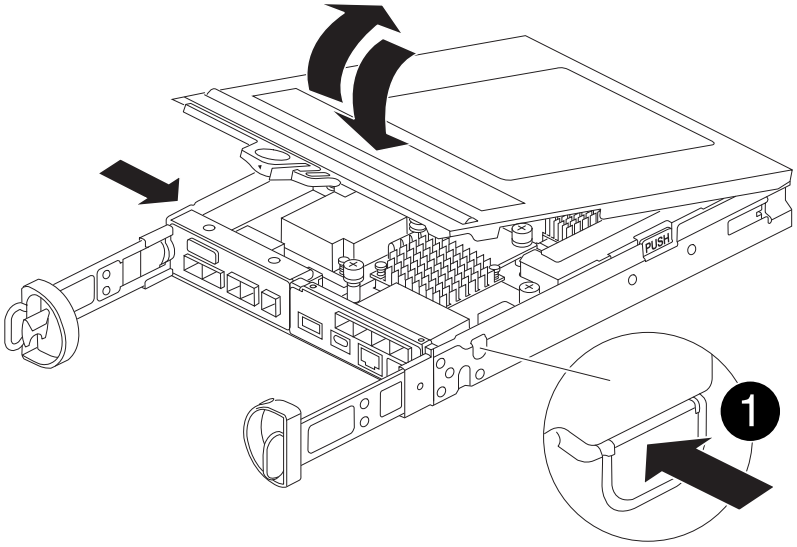
Steps

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

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.
3. Remove and set aside the cable management devices from the left and right sides of the controller module.
4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



1	Controller module cover release button

Step 3: Replace a caching module

Locate the caching module inside the controller, remove the failed caching module and replace it.

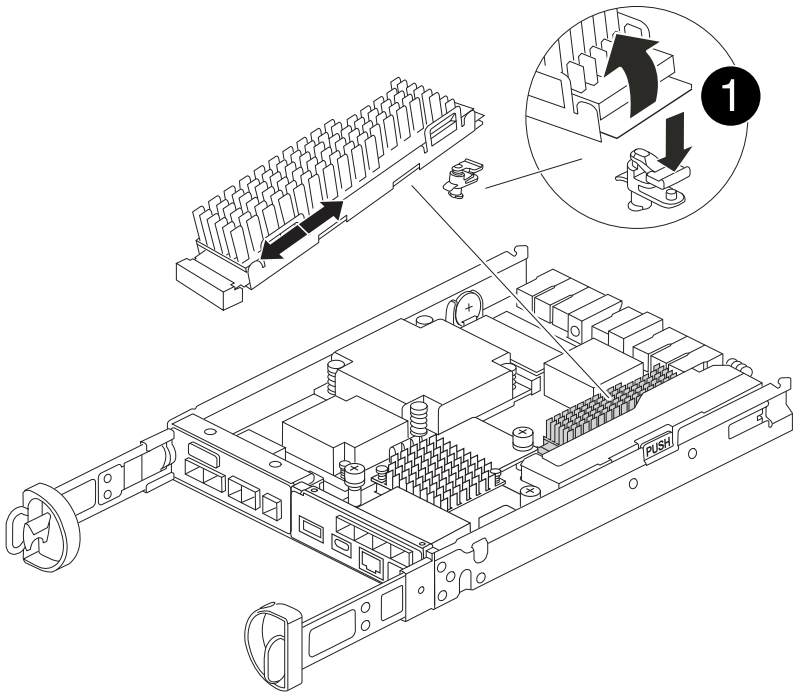
Animation - Replace the caching module

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module near the rear of the controller module and remove it.
   a. Press the blue release button and rotate the caching module upward.
   b. Gently pull the caching module straight out of the housing.



1	Caching module release button

3. Align the edges of the replacement caching module with the socket in the housing, and then gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Push the blue locking button, rotate the caching module all the way down, and then release the locking button to lock the caching module in place.
6. Reinstall the controller module cover and lock it into place.

Step 4: Reinstall the controller module

Reinstall the controller module into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Turn the controller module over and align the end with the opening in the chassis.
4. Gently push the controller module halfway into the system.

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

5. 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.

6. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.

Step 5: Restore automatic giveback and AutoSupport

Restore automatic giveback and AutoSupport if they have been disabled.

1. Restore automatic giveback by using the `storage failover modify -node local -auto -giveback true` command.
2. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END`

Step 6: Return the failed part to NetApp

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

Chassis

Overview of chassis replacement - FAS2820

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

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

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

Shut down the controllers - FAS2820

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

Before you begin

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

Steps

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

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

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

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

6. Exit the cluster shell:

   ```
   exit
   ```

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

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

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

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

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

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

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

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

Move and replace hardware - FAS2820

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

Step 1: Move a power supply

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

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

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

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

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

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

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

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

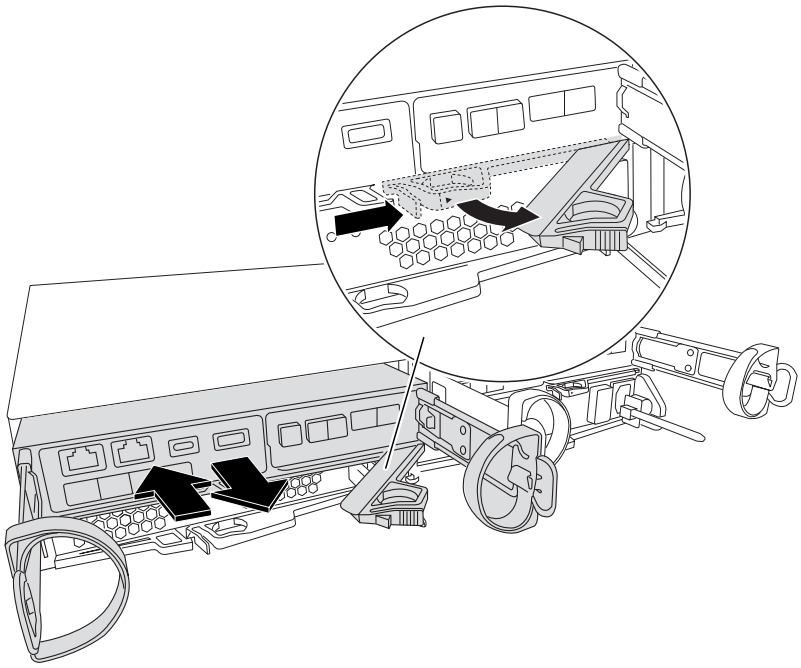
Step 2: Remove the controller module

Remove the controller module or modules from the impaired chassis.

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

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

2. Remove and set aside the cable management devices from the left and right sides of the controller module.
3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



4. Set the controller module aside in a safe place.
5. Repeat these steps for the second controller module in the chassis.

Step 3: Move drives to the replacement chassis

Move the drives from each drive bay opening in the impaired chassis to the same bay opening in the replacement chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button on the opposite side of 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 impaired chassis with the same bay opening in the replacement chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate to the closed position.

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

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

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

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

Remove the existing chassis from the equipment rack or system cabinet and install the replacement chassis in the equipment rack or system cabinet.

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

Step 5: Install the controller

Install the controller module and any other components into the replacement chassis, boot it tto Maintenance mode.

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

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

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

2. Recable the console to the controller module, and then reconnect the management port.
3. Repeat the preceding steps for the second controller in the replacement chassis.
4. Complete the installation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
   d. Repeat the preceding steps for the second controller module in the replacement chassis.

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

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

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

Restore and verify the configuration - FAS2820

Verify the HA state of the chassis bring up the system,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 based on the system's existing configuration: `ha-config modify chassis` *`ha-state`*

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

      - `ha`
      - `non-ha`

   b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. Exit Maintenance mode: `halt`. The LOADER prompt appears.
5. Boot the controller modules.

Step 2: Bring up the system

1. If you have not done so, plug the power cables back into the PSUs.
2. Turn on the PSUs by toggling the rocker switched to **ON**, and wait for the controllers to power up completely.
3. Check the front and the back of the chassis and controllers for any fault lights after power up.
4. Connect to the SP or BMC IP address of the nodes via SSH. This will be the same address used to shut down the nodes.

5. Perform additional health checks as described in How_to_perform_a_cluster_health_check_with_a_script_in_ONTAP
6. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

As a best practice, you should do the following:

- Resolve any Active IQ Wellness Alerts and Risks (Active IQ will take time to process post-power up AutoSupports - expect a delay in results)
- Run Active IQ Config Advisor
- Check system health using How_to_perform_a_cluster_health_check_with_a_script_in_ONTAP

Step 3: Return the failed part to NetApp

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

Controller

Overview of controller module replacement - FAS2820

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

- All drive shelves must be working properly.
- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system’s configuration.

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

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

Shut down the impaired controller - FAS2820

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

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

Steps

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

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

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

Replace the controller module hardware - FAS2820

Replace the impaired controller module hardware by removing the impaired controller, moving FRU components to the replacement controller module, installing the replacement controller module in the chassis, and then booting the replacement controller module.

Animation - Replace a controller module

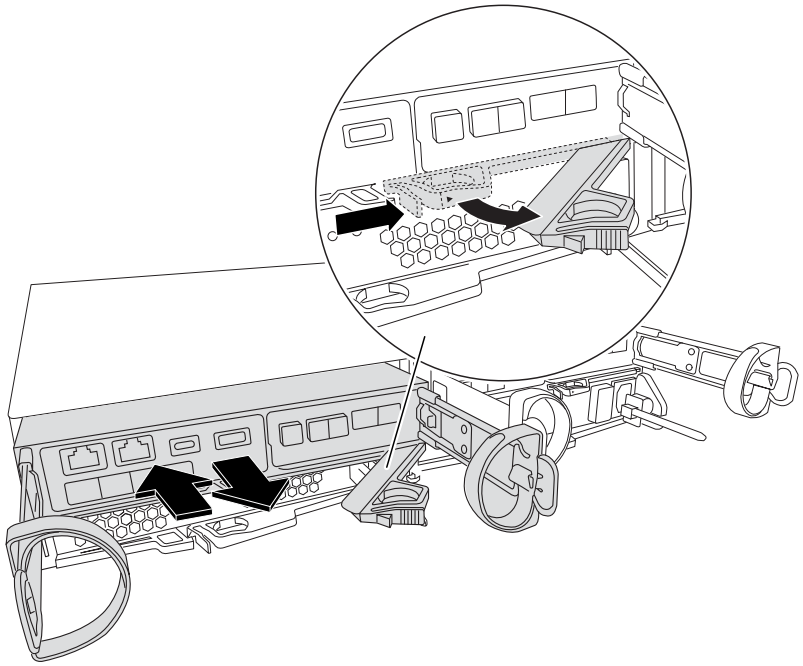
Step 1: Remove controller module

Remove the impaired controller module from the chassis.

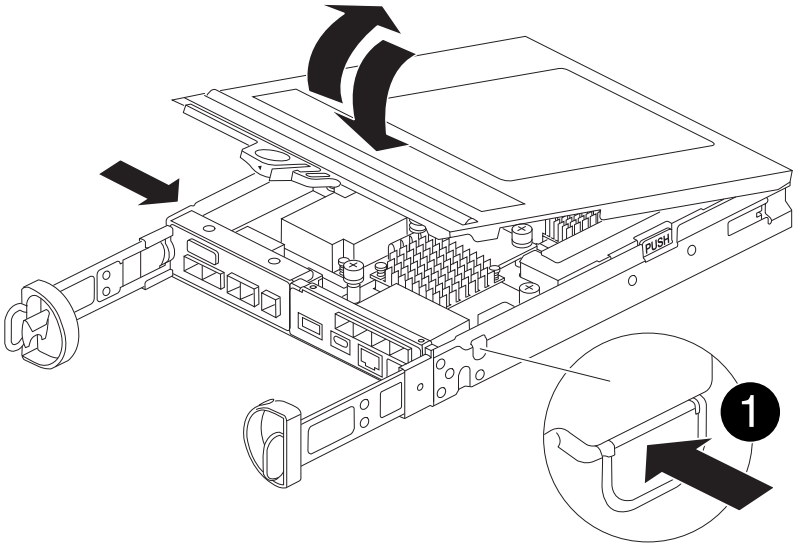
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

3. Remove and set aside the cable management devices from the left and right sides of the controller module.
4. If you left the SFP modules in the system after removing the cables, move them to the replacement controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



6. Turn the controller module over and place it on a flat, stable surface.
7. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.

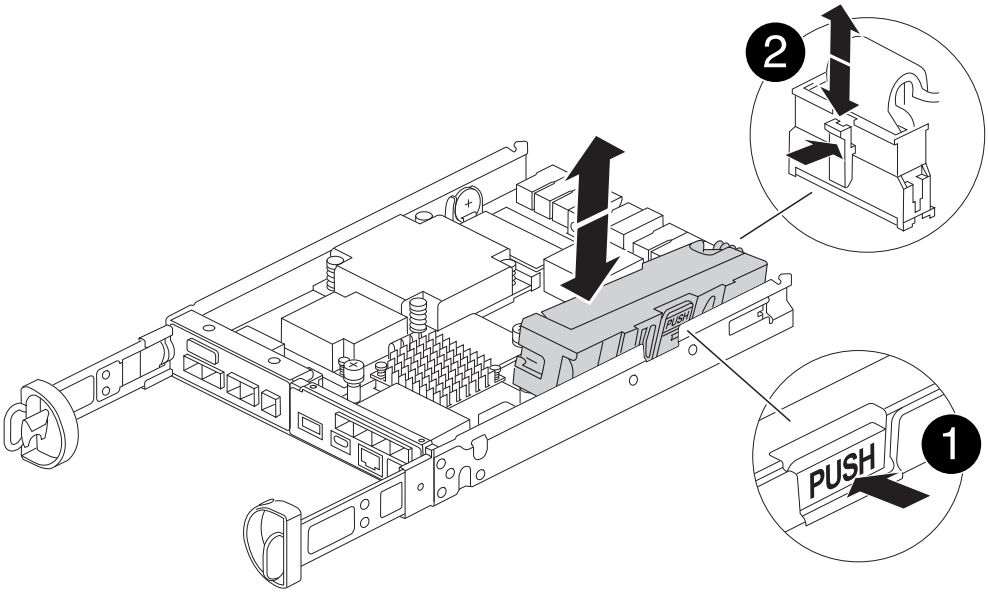


1	Controller module cover release button

Step 2: Move the NVMEM battery

Remove the NVMEM battery from the impaired controller module and install it into the replacement controller module.

Do not plug the NVMEM battery in until directed to do so.



1	NVMEM battery release button
2	NVMEM battery plug

1. Remove the battery from the controller module:

a. Press the blue button on the side of the controller module.

b. Slide the battery up until it clears the holding brackets, and then lift the battery out of the controller module.

c. Unplug the battery plug by squeezing the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.

2. Move the battery to the replacement controller module and install it:

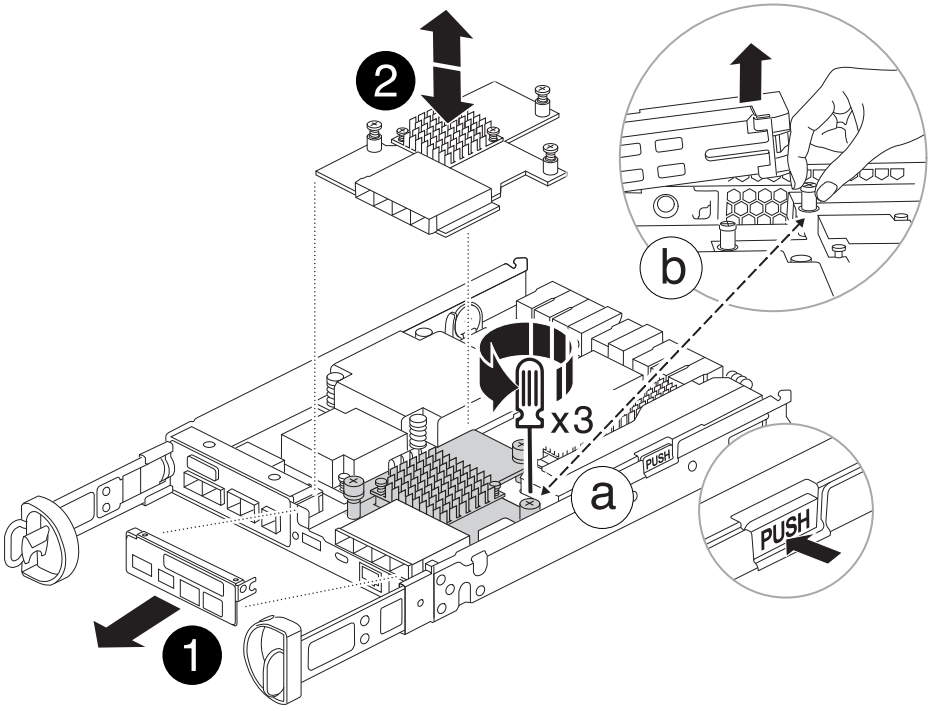
a. Aligning the battery with the holding brackets on the sheet metal side wall.

b. Slide the battery pack down until the battery latch engages and clicks into the opening on the side wall.

> Do not plug the battery in yet. You will plug it in once the rest of the components are moved to the replacement controller module.

Step 3: Remove the mezzanine card

Remove the IO Plate and PCIe mezzanine card from the impaired controller module.



1	IO Plate
2	PCIe mezzanine card

1. Remove the IO Plate by sliding it straight out from the controller module.
2. Loosen the thumbscrews on the mezzanine card.

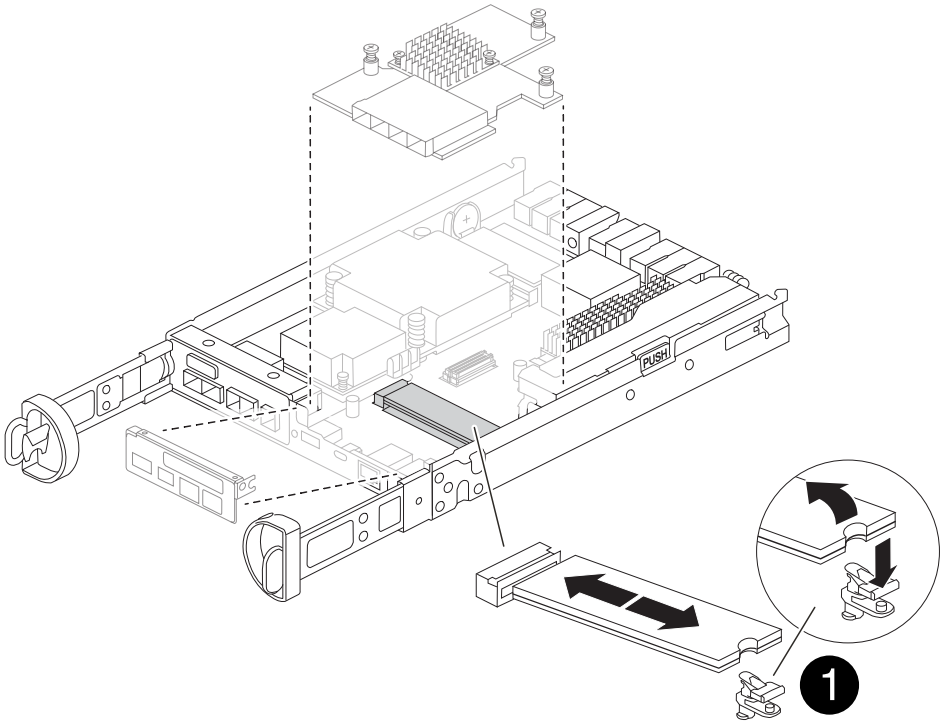
> You can loosen the thumbscrews with your fingers or a screwdriver.

3. Lift the mezzanine card straight up and set it aside on an anti-static surface.

Step 4: Move the boot media

Remove the boot media from the impaired controller module and install it in the replacement controller module.

1. After removing the mezzanine card, locate the boot media using the following illustration or the FRU map on the controller module:



1	Boot media release button

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

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

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

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

   c. Push the blue locking button on the boot media housing, rotate the boot media all the way down, and then release the locking button to lock the boot media in place.

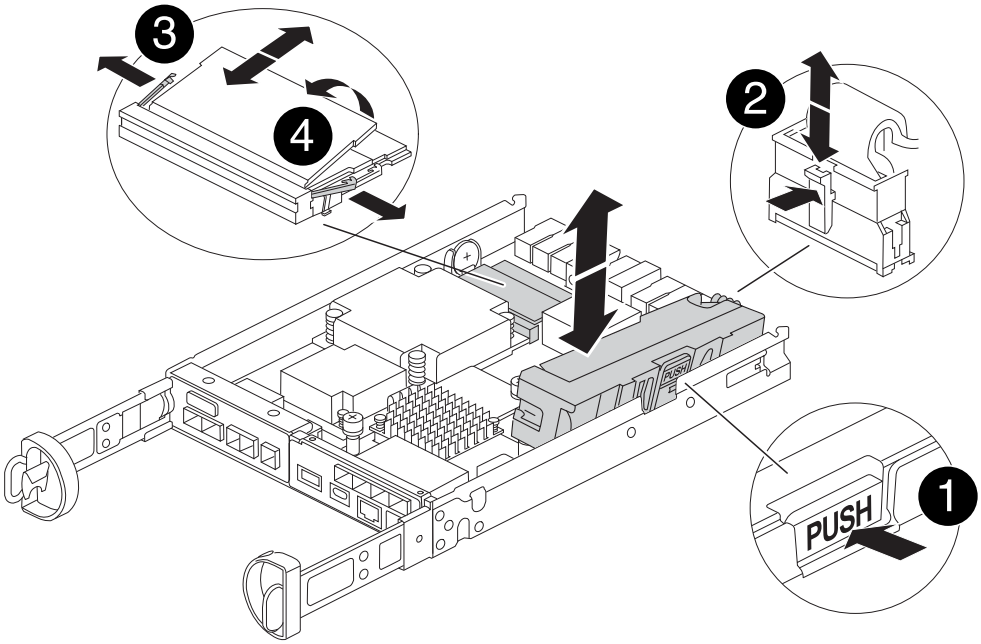
Step 5: Install the mezzanine card in the replacement controller

Install the mezzanine card in the replacement controller module.

1. Reinstall the mezzanine card:
   a. Align mezzanine card with the socket on the motherboard.
   b. Gently push down on the card to seat the card in the socket.
   c. Tighten the three thumbscrews on the mezzanine card.
2. Reinstall the IO Plate.

Step 6: Move the DIMMs

Remove the DIMMs from the impaired controller module and install them into the replacement controller module.



1	DIMM locking latches
2	DIMM

1. Locate the DIMMs on your controller module

   Note the location of the DIMM in the sockets so that you can insert the DIMM in the same location in the replacement controller module and in the proper orientation.

2. Remove the DIMMs from the impaired controller module:
   a. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM.

      The DIMM will rotate up a little.

   b. Rotate the DIMM as far as it will go, and then slide the DIMM out of the socket.

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

3. Verify that the NVMEM battery is not plugged into the replacement controller module.
4. Install the DIMMs in the replacement controller in the same place they were in the impaired controller:
   a. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

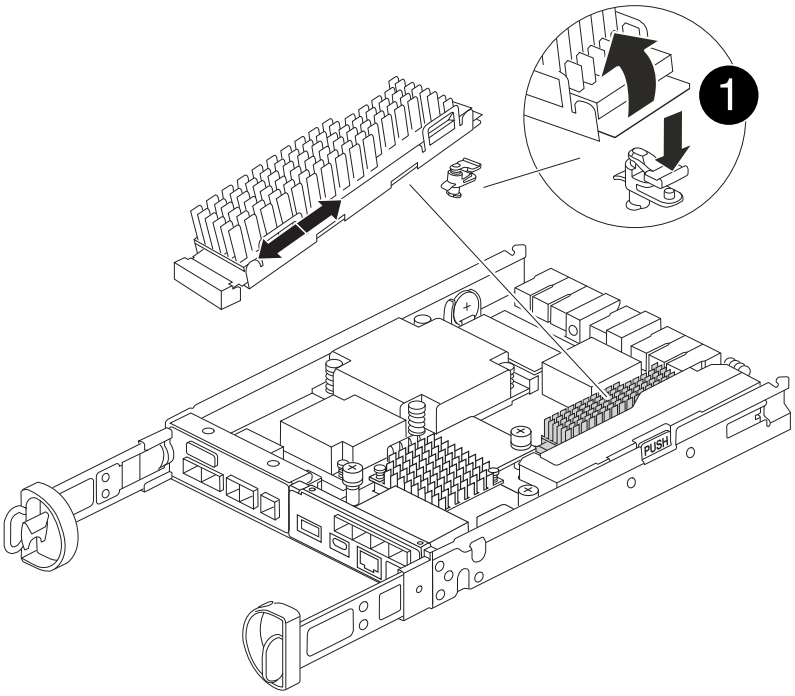
      The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

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

5. Repeat these steps for the other DIMM.

Step 7: Move a caching module

Remove the caching module from the impaired controller module install it into replacement controller module.



1	Caching module locking button

1. Locate the caching module near the rear of the controller module and remove it:
   a. Press the blue locking button and rotate the caching module upward.
   b. Gently pull the caching module straight out of the housing.
2. Install the caching module in the replacement controller module:
   a. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.

b. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

c. Push the blue locking button, rotate the caching module all the way down, and then release the locking button to lock the caching module in place.

3. Plug in the NVMEM battery.

   Make sure that the plug locks down into the battery power socket on the motherboard.

   If plugging in the battery is difficult, remove the battery from the controller module, plug it in, and then reinstall the battery into the controller module.

4. Reinstall the controller module cover.

Step 8: Install the NV battery

Install the NV battery into the replacement controller module.

1. Plug the battery plug back into the socket on the controller module.

   Make sure that the plug locks down into the battery socket on the motherboard.

2. Aligning the battery with the holding brackets on the sheet metal side wall.
3. Slide the battery pack down until the battery latch engages and clicks into the opening on the side wall.
4. Reinstall the controller module cover and lock it into place.

Step 9: Install the controller

Install the replacement controller module into the system chassis and boot ONTAP.

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

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Turn the controller module.
4. 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.

5. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

b. If you have not already done so, reinstall the cable management device.

c. Bind the cables to the cable management device with the hook and loop strap.

> You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete. If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the `update_flash` command, and then enter `bye -g` to reboot the system.

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

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

Restore and verify the system configuration - FAS2820

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

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

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

About this task

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

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

Steps

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

   The date and time are based on the configured timezone.

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

   The date and time are given in GMT.

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

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

   The date and time are given in GMT.

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

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

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

   The HA state should be the same for all components.

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

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

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`

     a. Confirm that the setting has changed: `ha-config show`

3. Reboot the controller module.

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

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

Recable the system and reassign disks - FAS2820

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

Step 1: Recable the system

Verify the controller module's storage and network connections by using Active IQ Config Advisor.

Steps

1. Download and install Config Advisor.
2. Enter the information for the target system, and then click Collect Data.
3. 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.

4. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

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

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

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

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

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

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

   b. Save any coredumps: `system node run -node` *`local-node-name`* `partner savecore`
   c. Wait for the `savecore` command to complete before issuing the giveback.

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

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

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

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

> If the giveback is vetoed, resolve the veto issue. If the veto is not critical to resolve, you can override the veto.

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

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

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

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

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

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

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

Complete system restoration - FAS2820

Restore your system to full operation by restoring the NetApp Storage Encryption or Volume Encryption configurations (if necessary), and installing licenses for the replacement controller, and returning the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Install licenses for the replacement controller in ONTAP

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

About this task

Until you install license keys, features requiring standard licenses continue to be available to the *replacement* node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed.

Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the *replacement* node as soon as possible.

Before you begin

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

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

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

Steps

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

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

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

Step 2: Verify LIFs and register the serial number

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

Steps

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

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

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. Check the health of your cluster. See the How to perform a cluster health check with a script in ONTAP KB article for more information.

4. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.
5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 3: Return the failed part to NetApp

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

Replace a DIMM - FAS2820

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

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

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

Animation - Replace a DIMM

Step 1: Shut down the impaired controller

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

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

Steps

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

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

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

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

Step 2: Remove controller module

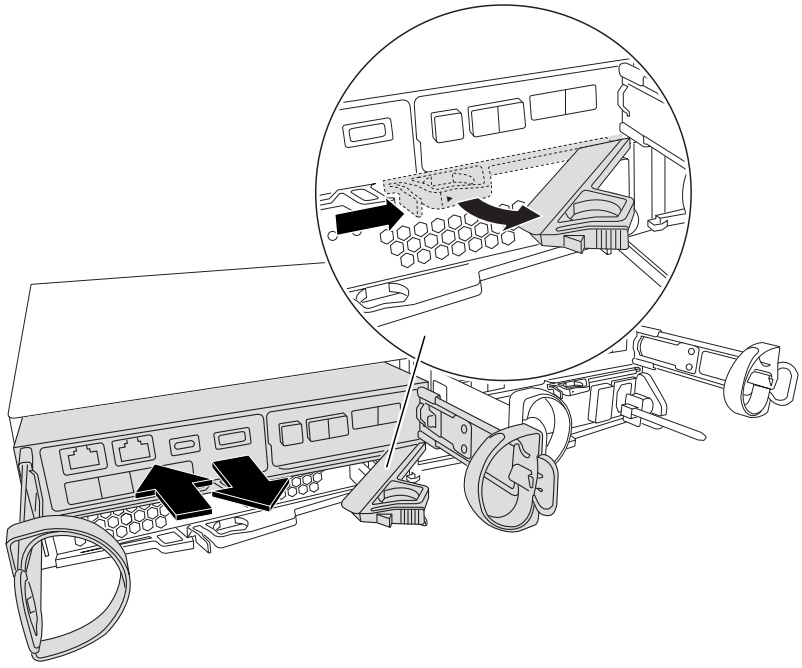
Remove the controller module from the system and then remove the controller module cover.

Steps

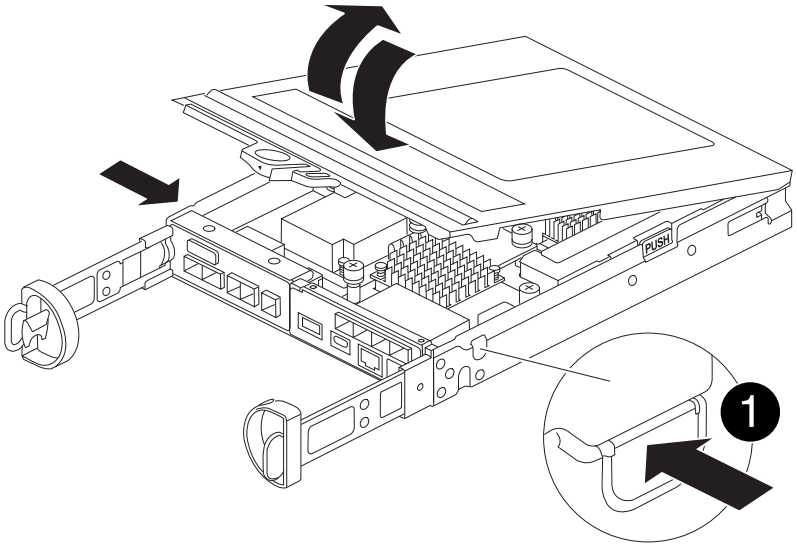
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

3. Remove and set aside the cable management devices from the left and right sides of the controller module.
4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



1	Controller module cover release button

Step 3: Replace the DIMMs

Locate the DIMM inside the controller, remove it, and replace it.

Before replacing a DIMM, you need to unplug the NVMEM battery from the controller module.

Steps

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

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

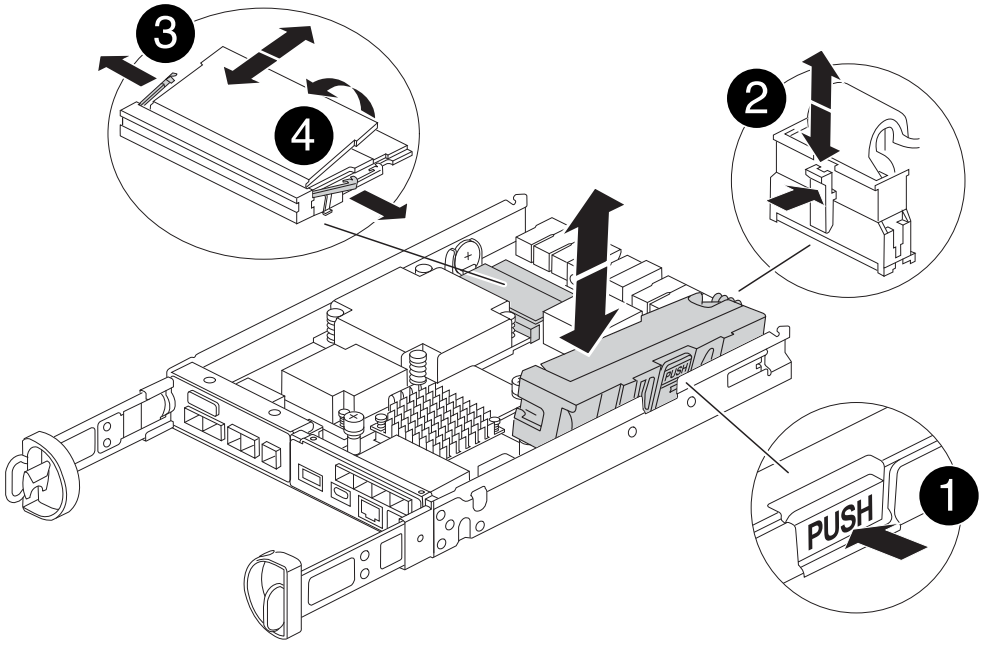
2. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
3. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:
   a. Remove the battery from the controller module by pressing the blue button on the side of the controller module.
   b. Slide the battery up until it clears the holding brackets, and then lift the battery out of the controller module.
   c. Locate the battery cable, press the clip on the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.
   d. Confirm that the NVMEM LED is no longer lit.
   e. Reconnect the battery connector and recheck the LED on the back of the controller.
   f. Unplug the battery cable.

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

   The DIMM will rotate up a little.

7. Rotate the DIMM as far as it will go, and then slide the DIMM out of the socket.

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



1	NVRAM battery release button
2	NVRAM battery plug
3	DIMM ejector tabs
4	DIMMs

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

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

9. Insert the DIMM squarely into the slot.

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

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

10. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
11. Reconnect the NVMRM battery:
    a. Plug in the NVRAM battery.

       Make sure that the plug locks down into the battery power socket on the motherboard.

    b. Align the battery with the holding brackets on the sheet metal side wall.
    c. Slide the battery pack down until the battery latch engages and clicks into the opening on the side wall.
12. Reinstall the controller module cover.

Step 4: Reinstall the controller module

Reinstall the controller module into the chassis.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Turn the controller module over and align the end with the opening in the chassis.
4. Gently push the controller module halfway into the system.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.

5. 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.

6. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
7. Reboot the controller module.

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

   - A prompt warning of a system ID mismatch and asking to override the system ID.

- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down. You can safely respond `y` to these prompts.

Step 5: Restore automatic giveback and AutSupport

Restore automatic giveback and AutoSupport if they have been disabled.

1. Restore automatic giveback by using the `storage failover modify -node local -auto -giveback true` command.
2. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

Step 6: Return the failed part to NetApp

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

Replace SSD Drive or HDD Drive - FAS2820

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

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

Before you begin

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

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

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

- Determine whether SED authentication is enabled.

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

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

About this task

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

versions.

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

Option 1: Replace SSD

Steps

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment, if it is enabled.
   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.
2. Properly ground yourself.
3. Physically identify the failed drive.

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

   The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.
4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.
6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the midplane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.
7. Verify that the drive’s activity (green) LED is illuminated.

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

8. If you are replacing another drive, repeat the preceding steps.
9. If you disabled automatic drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives:

      `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive:

      `storage disk assign -disk disk_name -owner node_name`

      You can enter the command on either controller module.

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

   c. Reenable automatic drive assignment if needed:

      `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.
10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact NetApp Support if you need the RMA number or additional help with the replacement procedure.

Option 2: Replace HDD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.
2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive

5. Press the release button on the disk drive face.

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

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

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

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

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

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

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

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

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

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

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

       You can enter the command on either controller module.

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

       You can enter the command on either controller module.

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

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

You must reenable automatic drive assignment on both controller modules.

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

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

Replace the NVMEM battery - FAS2820

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 NetApp Support.

Step 1: Shut down the impaired controller

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

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

Steps

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

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

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`

3. Take the impaired controller to the LOADER prompt:

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

Step 2: Remove and open the controller module

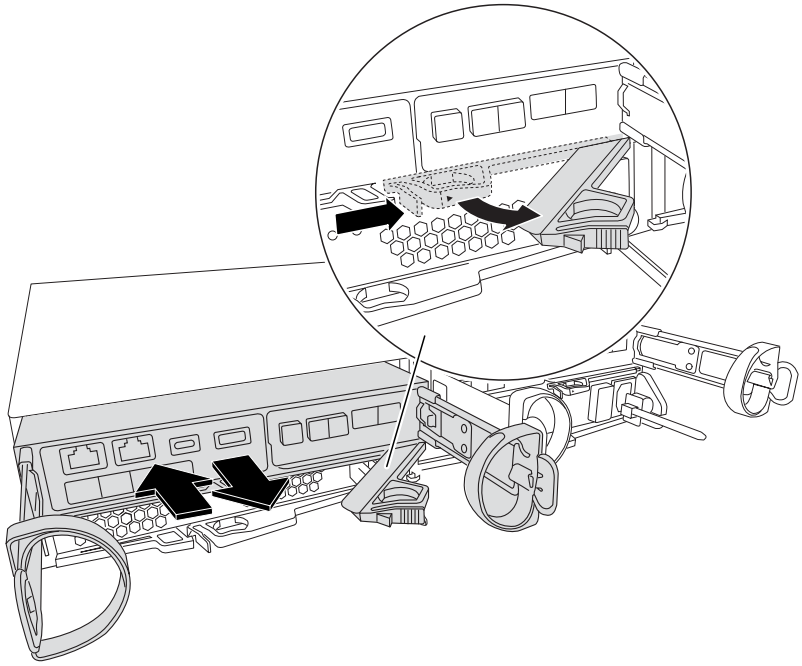
Remove and open the controller module.

Steps

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

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

3. Remove and set aside the cable management devices from the left and right sides of the controller module.
4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module half-way out of the chassis.



5. Check the NVMEM LED located on the back of the controller module. Look for the NV icon:

The green NV LED on the faceplate will start flashing when power is removed from the controller if the system was in the "waiting for giveback" state, or the system was not taken over or halted properly (uncommitted data). If the impaired controller module was not successfully taken over by the partner controller module, contact NetApp Support

   - If the green NV status LED begins flashing when the controller module is removed from the chassis:
     - Confirm that the controller had a clean takeover by the partner controller module or the impaired controller shows *waiting for giveback*, the flashing LED can be ignored and you can complete removing the impaired controller from the chassis.

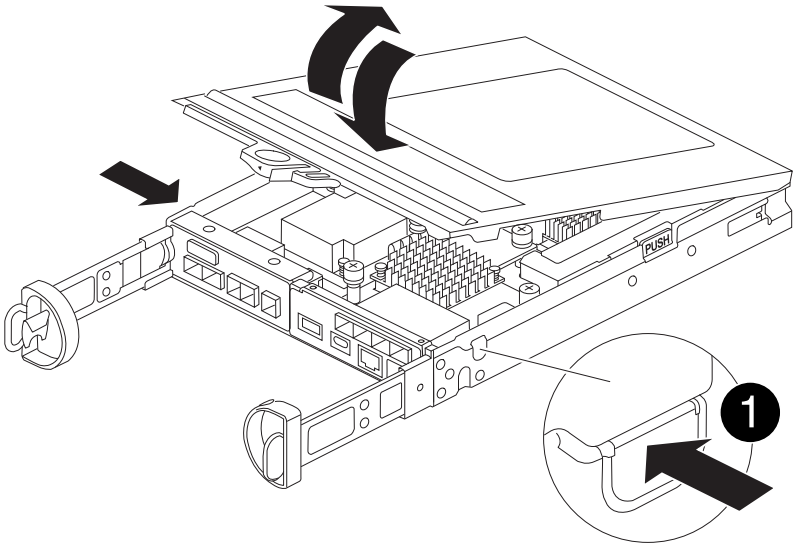
◦ If the green NV LED if off, you can complete removing the impaired controller from the chassis.

Step 3: Replace the NVMEM battery

Remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

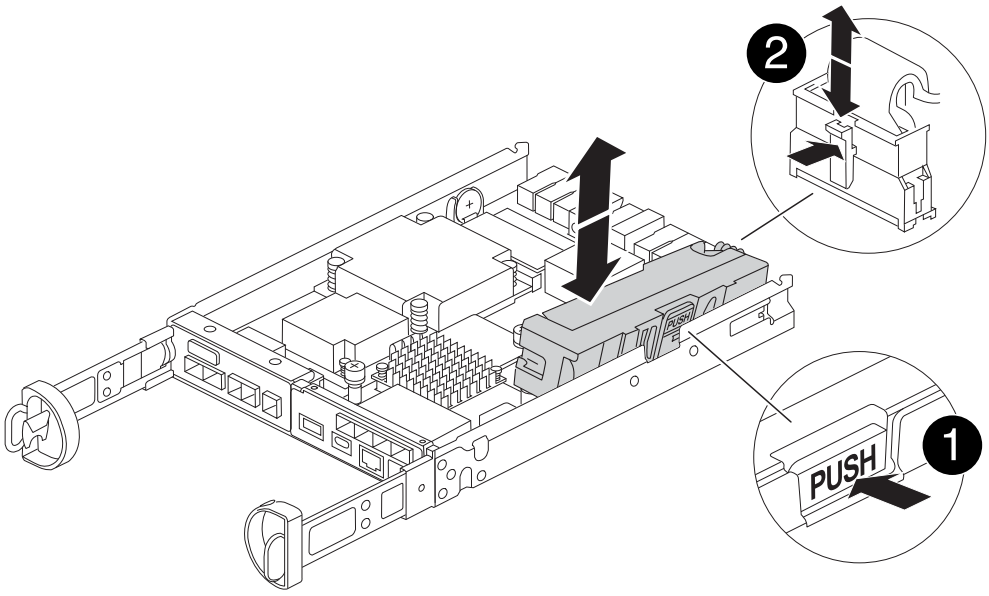
Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the controlle module from the chassis.
3. Turn the controller module over and place it on a flat, stable surface.
4. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



5. Locate the NVMEM battery in the controller module.

Animation - Replace the NV battery



1	Battery release tab
2	Battery power connector

6. Remove the failed battery from the controller module:
   a. Press the blue button on the side of the controller module.
   b. Slide the battery up until it clears the holding brackets, and then lift the battery out of the controller module.
   c. Unplug the battery from the controller module
7. Remove the replacement battery from its package. Install the replacement battery:
   a. Plug the battery plug back into the socket on the controller module.

      Make sure that the plug locks down into the battery socket on the motherboard.

   b. Aligning the battery with the holding brackets on the sheet metal side wall.
   c. Slide the battery pack down until the battery latch engages and clicks into the opening on the side wall.
8. Reinstall the controller module cover and lock it into place.

Step 4: Reinstall the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Turn the controller module over and align the end with the opening in the chassis.
4. 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.

5. 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.

6. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   b. If you have not already done so, reinstall the cable management device.

c. Bind the cables to the cable management device with the hook and loop strap.

7. Reboot the controller module.

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

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

Step 5: Restore automatic giveback and AutSupport

Restore automatic giveback and AutoSupport if they have been disabled.

1. Restore automatic giveback by using the `storage failover modify -node local -auto -giveback true` command.
2. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

Step 6: Return the failed part to NetApp

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

Replace a mezzanine card - FAS2820

Replace the mezzanine card by disconnecting the cables and any SFP and QSFP modules from the card, replace the failed mezzanine card, and then recable the cards.

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

Animation - Replace the mezzanine card

Step 1: Shut down the impaired controller

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

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

Steps

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

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

2. If the impaired controller is part of an HA pair, disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

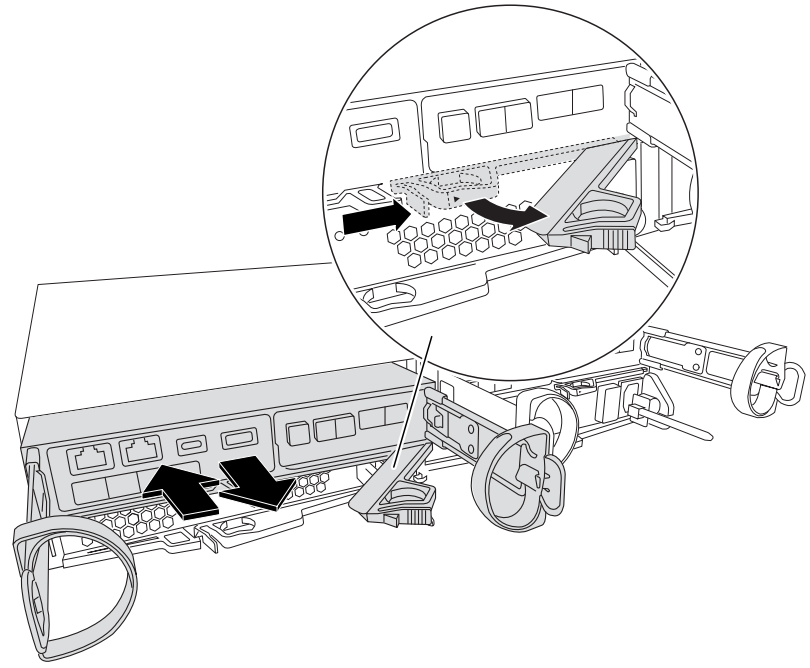
Step 2: Remove the controller module

Remove the controller module from the system and then remove the cover on the controller module.

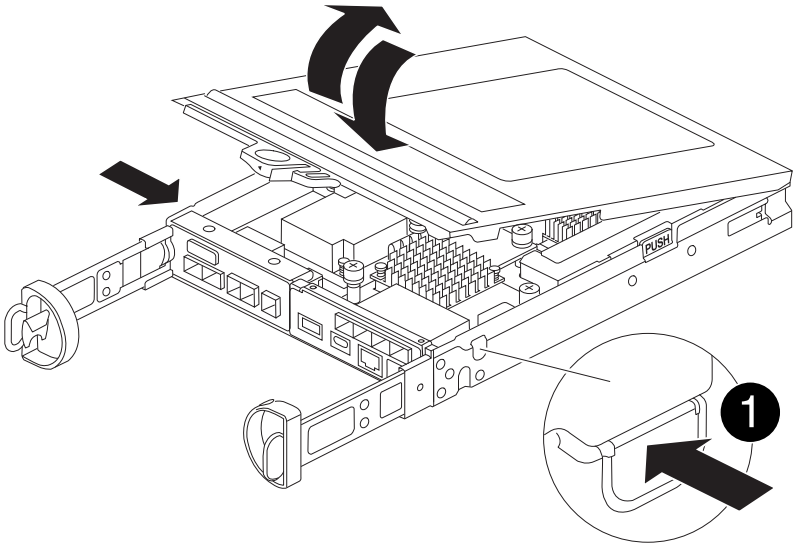
Steps

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

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.
3. Remove and set aside the cable management devices from the left and right sides of the controller module.
4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.

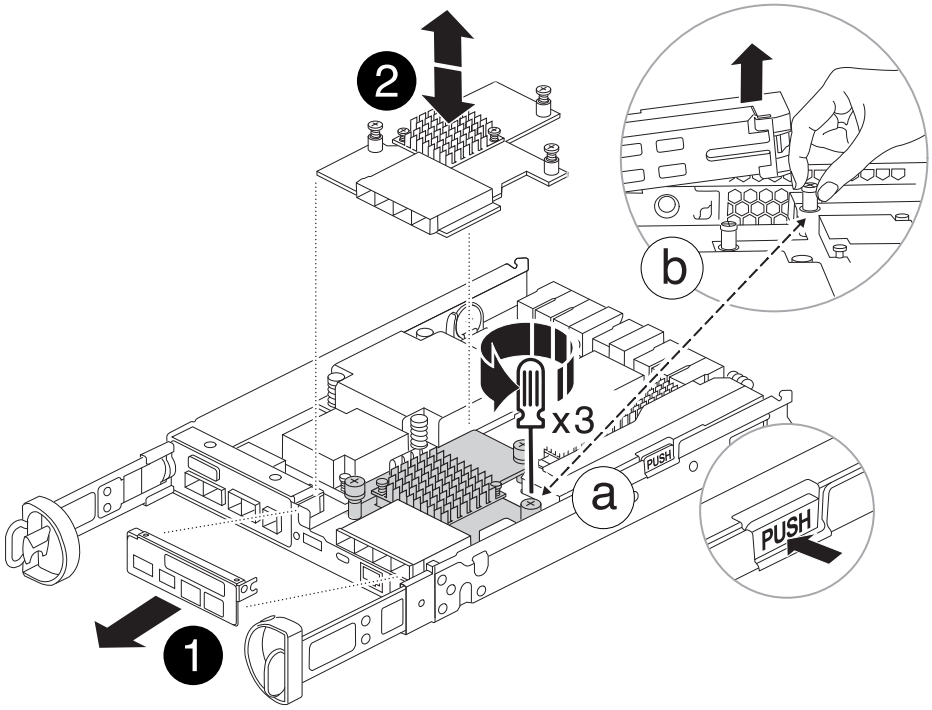


1	Controller module cover release button

Step 3: Replace the mezzanine card

Replace the mezzanine card.

1. If you are not already grounded, properly ground yourself.
2. Remove the mezzanine card using the following illustration or the FRU map on the controller module:



1	IO Plate
2	PCIe mezzanine card

a. Remove the IO Plate by sliding it straight out from thr controller module.

b. Loosen the thumbscrews on the mezzanine card and lift the mezzanine card straight up.

> You can loosen the thumbscrews with your fingers or a screwdriver. If you use your fingers, you might need to rotate the NV battery up for better finger purchase on the thumbscrew next to it.

3. Reinstall the mezzanine card:

   a. Align the socket on the replacement mezzanine card plug with the socket on the motherboard, and then gently seat the card squarely into the socket.

   b. Tighten the three thumbscrews on the mezzanine card.

   c. Reinstall the IO Plate.

4. Reinstall the controller module cover and lock it into place.

Step 4: Install the controller module

Reinstall the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Turn the controller module over and align the end with the opening in the chassis.

4. Gently push the controller module halfway into the system.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.

5. 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.

6. Complete the reinstallation of the controller module:
   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

   b. If you have not already done so, reinstall the cable management device.
   c. Bind the cables to the cable management device with the hook and loop strap.
7. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
8. Restore automatic giveback by using the `storage failover modify -node local -auto -giveback true` command.
9. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

Step 5: Return the failed part to NetApp

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

Swap out a power supply - FAS2820

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

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

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

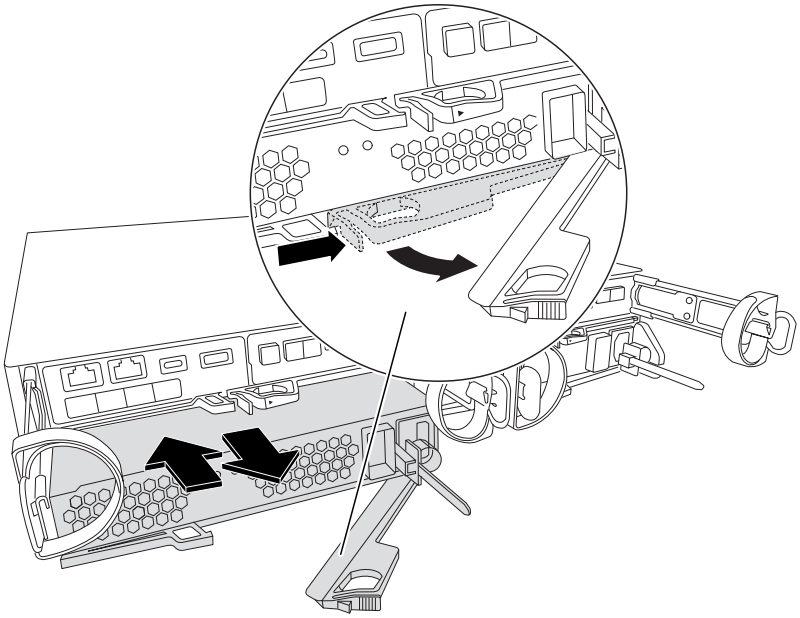
  It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- Power supplies are auto-ranging.

Animation - Replace power supply

Steps

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



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

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

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

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

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

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

b. Secure the power cable to the power supply using the power cable retainer.

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

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

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

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

Replace the real-time clock battery - FAS2820

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

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

Step 1: Shut down the impaired controller

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

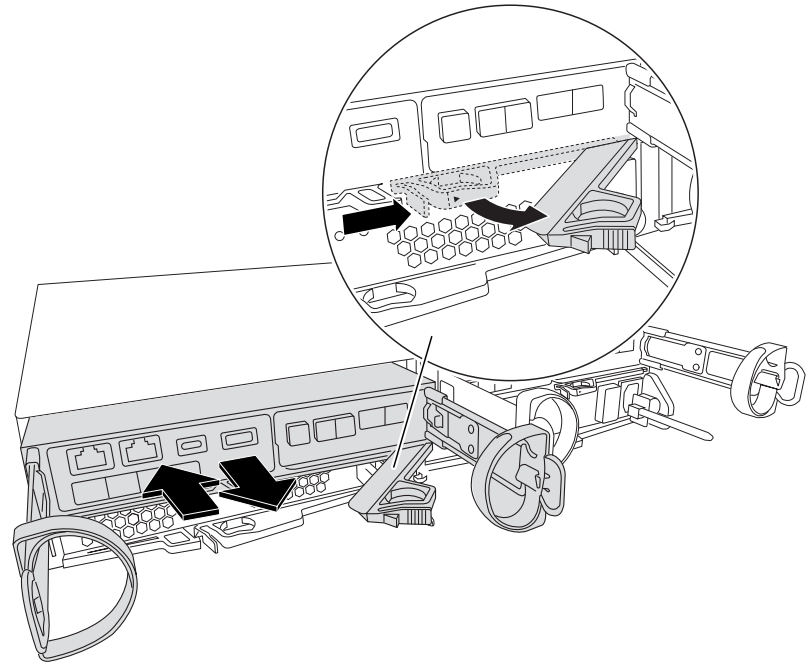
Step 2: Remove controller module

Remove the controller module from the system and then remove the cover on the controller module.

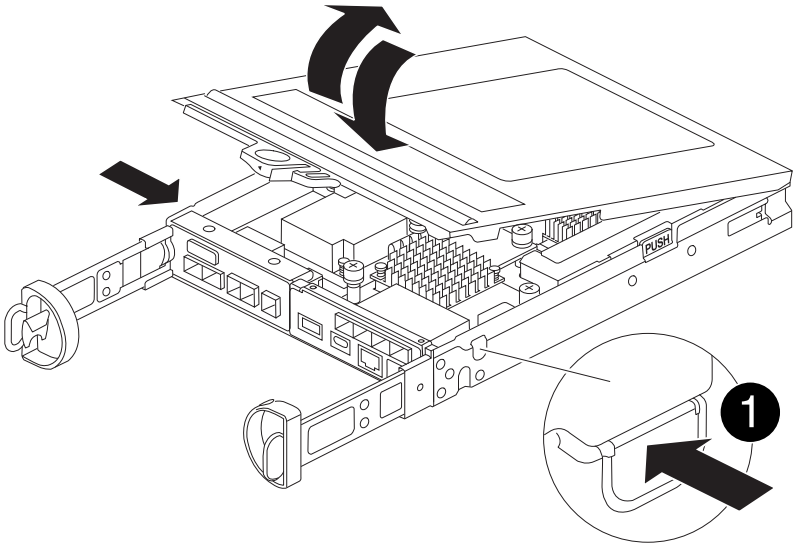
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

3. Remove and set aside the cable management devices from the left and right sides of the controller module.
4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



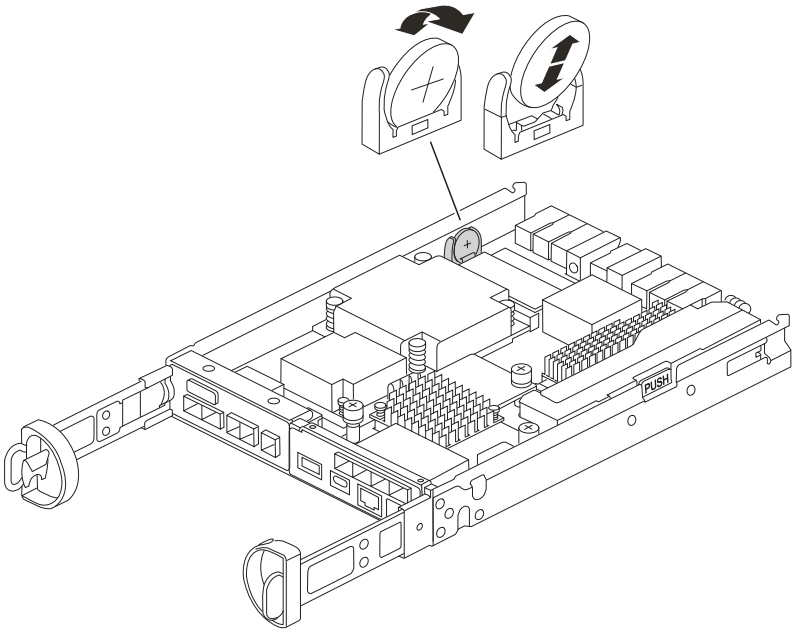
5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



Step 3: Replace the RTC battery

Replace the RTC battery by locating it inside the controller and follow the specific sequence of steps.

Animation - Replace the RTC battery



1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.
3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.

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

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

Step 4: Reinstall the controller module

Reinstall the controller module and boot it to the LOADER prompt..

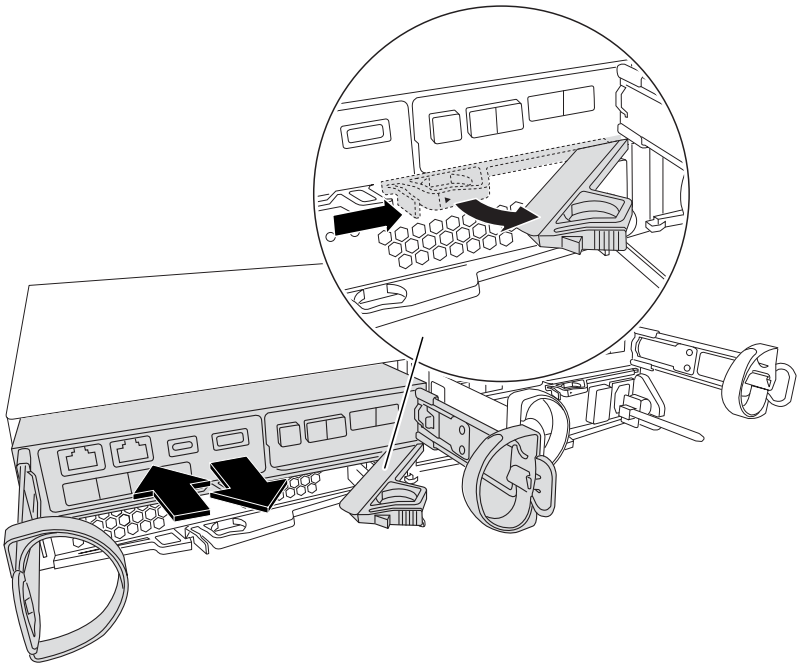
1. Turn the controller module over and align the end with the opening in the chassis.
2. Gently push the controller module halfway into the system.Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

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

3. Recable the system, as needed.

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

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:



a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

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

b. If you have not already done so, reinstall the cable management device.
c. Bind the cables to the cable management device with the hook and loop strap.
d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
e. Halt the controller at the LOADER prompt.

Step 5: Set time/date after RTC battery replacement

1. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
2. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
3. Return the controller to normal operation by giving back its storage: `storage failover giveback`

`-ofnode impaired_node_name`

4. Restore automatic giveback by using the `storage failover modify -node local -auto -giveback true` command.
5. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

Step 6: Return the failed part to NetApp

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

Key specifications for FAS2820

The following are select specifications for the FAS2820 storage system in a single high availability pair. Visit NetApp Hardware Universe for the complete specifications for this storage system.

Key specifications for FAS2820

- Platform Configuration: FAS2820 Single Chassis HA Pair
- Max Raw Capacity: 3.1680 PB
- Memory: 128.0000 GB
- Form Factor: 2U chassis with 2 HA controllers and 12 drive slots
- ONTAP Version: ONTAP: 9.16.1P2
- PCIe Expansion Slots: 4
- Minimum ONTAP Version: ONTAP 9.13.1RC1

Scaleout maximums

- Type: NAS; HA Pairs: 12; Raw Capacity: 38.0 PB / 33.8 PiB; Max Memory: 1536 GB
- Type: SAN; HA Pairs: 6; Raw Capacity: 19.0 PB / 16.9 PiB; Max Memory: 768 GB
- Type: HA Pair; Raw Capacity: 3.2 PB / 2.8 PiB; Max Memory: 128.0000

I/O

Onboard I/O

- Protocol: Ethernet 25 Gbps; Ports: 4
- Protocol: SAS 12 Gbps; Ports: 4

Total I/O

- Protocol: Ethernet 25 Gbps; Ports: 12
- Protocol: Ethernet 10 Gbps; Ports: 8
- Protocol: FC 32 Gbps; Ports: 8

- Protocol: NVMe/FC 32 Gbps; Ports: 8
- Ports: 0
- Protocol: SAS 12 Gbps; Ports: 4

Management ports

- Protocol: Ethernet 1 Gbps; Ports: 2
- Protocol: RS-232 115 Kbps; Ports: 4
- Protocol: USB 600 Mbps; Ports: 2

Storage networking supported

- CIFS
- FC
- FCoE
- iSCSI
- NFS v3
- NFS v4.0
- NFS v4.1
- NVMe/TCP
- S3
- S3 with NAS
- SMB 2.0
- SMB 2.1
- SMB 2.x
- SMB 3.0
- SMB 3.1
- SMB 3.1.1

System environment specifications

- Typical Power: 1815 BTU/hr
- Worst-case Power: 2339 BTU/hr
- Weight: 57.2 lb 25.9 kg
- Height: 2U
- Width: 19” IEC rack-compliant (17.6” 44.7 cm)
- Depth: 20.0” (25.1” with cable management bracket)
- Operating Temp/Altitude/Humidity: 10°C to 35°C (50°F to 95°F) at up to 3048m (10000 ft) elevation;8% to 80% relative humidity, noncondensing
- Non-operating Temp/Humidity: -40°C to 70°C (-40°F to 158°F) up to 12192m (40000 ft) 10% to 95% relative humidity, noncondensing, in original container

- Acoustic Noise: Declared sound power (LwAd): 7.8 Sound pressure (LpAm) (bystander positions): 68.4 dB

Compliance

- Certifications EMC/EMI: AMCA, FCC, ICES, KC, Morocco, VCCI
- Certifications safety: BIS, CB, CSA, G_K_U-SoR, IRAM, NOM, NRCS, SONCAP, TBS
- Certifications Safety/EMC/EMI: EAC, UKRSEPRO
- Certifications Safety/EMC/EMI/RoHS: BSMI, CE DoC, UKCA DoC
- Standards EMC/EMI: BS-EN-55024, BS-EN55035, CISPR 32, EN55022, EN55024, EN55032, EN55035, EN61000-3-2, EN61000-3-3, FCC Part 15 Class A, ICES-003, KS C 9832, KS C 9835
- Standards Safety: ANSI/UL60950-1, ANSI/UL62368-1, BS-EN62368-1, CAN/CSA C22.2 No. 60950-1, CAN/CSA C22.2 No. 62368-1, CNS 14336, EN60825-1, EN62368-1, IEC 62368-1, IEC60950-1, IS 13252(part 1)

High availability

- Ethernet based baseboard management controller (BMC) and ONTAP management interface
- Redundant hot-swappable controllers
- Redundant hot-swappable power supplies
- SAS in-band management over SAS connections for external shelves

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.