Maintain

Install and maintain

NetApp
May 20, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems/asa-c250/maintain-overview.html on May 20, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Maintain 1
Maintain ASA C250 hardware 1
Boot media 2

Maintain

Maintain ASA C250 hardware

For the ASA C250 storage system, you can perform maintenance procedures on the following components.

Boot media

The boot media stores a primary and secondary set of boot image files that the system uses when it boots.

Chassis

The chassis is the physical enclosure housing all the controller components such as the controller/CPU unit, power supply, and I/O.

Controller

A controller consists of a board, firmware, and software. It controls the drives and implements the ONTAP functions.

DIMM

You must replace a DIMM (dual in-line memory module) when a memory mismatch is present, or you have a failed DIMM.

Drive

A drive is a device that provides the physical storage media for data.

Fan

The fan cools the controller.

Mezzanine card

A Mezzanine card is a printed circuit board that plugs directly into another plug-in card.

NVEM battery

A battery is included with the controller and preserves cached data if the AC power fails.

Power supply

A power supply provides a redundant power source in a controller shelf.

Real-time clock battery

A real time clock battery preserves system date and time information if the power is off.

Boot media

Overview of boot media replacement - ASA C250

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots.

Before you begin

- You must have a USB flash drive, formatted to MBR/FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.
- You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

About this task

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

Check onboard encryption keys - ASA C250

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

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

Steps

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

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

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

Check NVE or NSE on systems running ONTAP 9.6 and later

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

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

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

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

Verify NVE configuration

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

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

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

the OKM information:

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

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

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

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

e. Shut down the impaired controller.

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

a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

If the command fails, contact NetApp Support.

mysupport.netapp.com

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

c. Shut down the impaired controller.

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

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

Enter the customer's 32 character, alphanumeric onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.
mysupport.netapp.com

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

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

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

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

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

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

h. You can safely shut down the controller.

Verify NSE configuration

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

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

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

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

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

      Enter the customer's 32 character, alphanumeric onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

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

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

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

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

h. You can safely shut down the controller.

Shut down the controller - ASA C250

Option 1: Most systems

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

Option 2: Systems in a MetroCluster

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

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

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

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

impaired controller; see Synchronize a node with the cluster.

- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

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

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

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

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

Replace the boot media - ASA C250

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

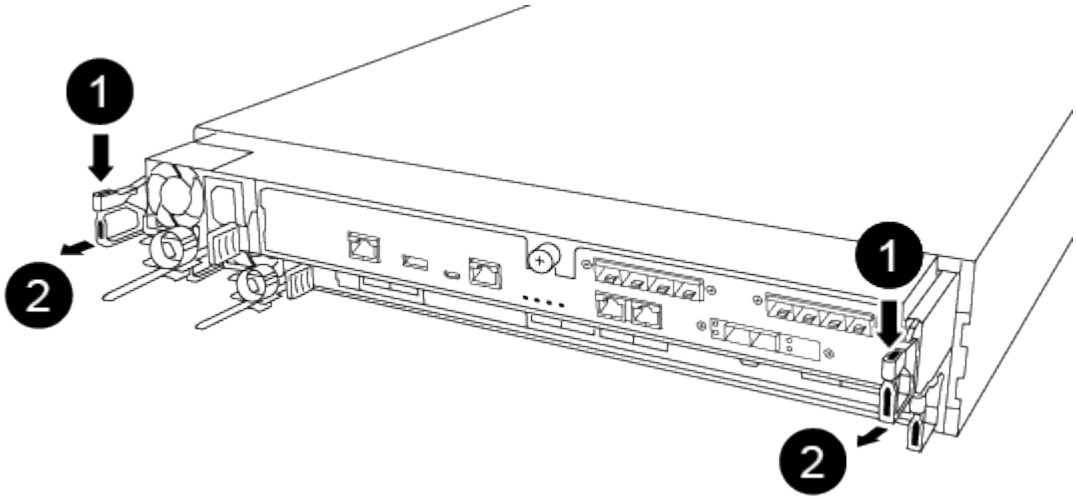
Step 1: Remove the controller module

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

Steps

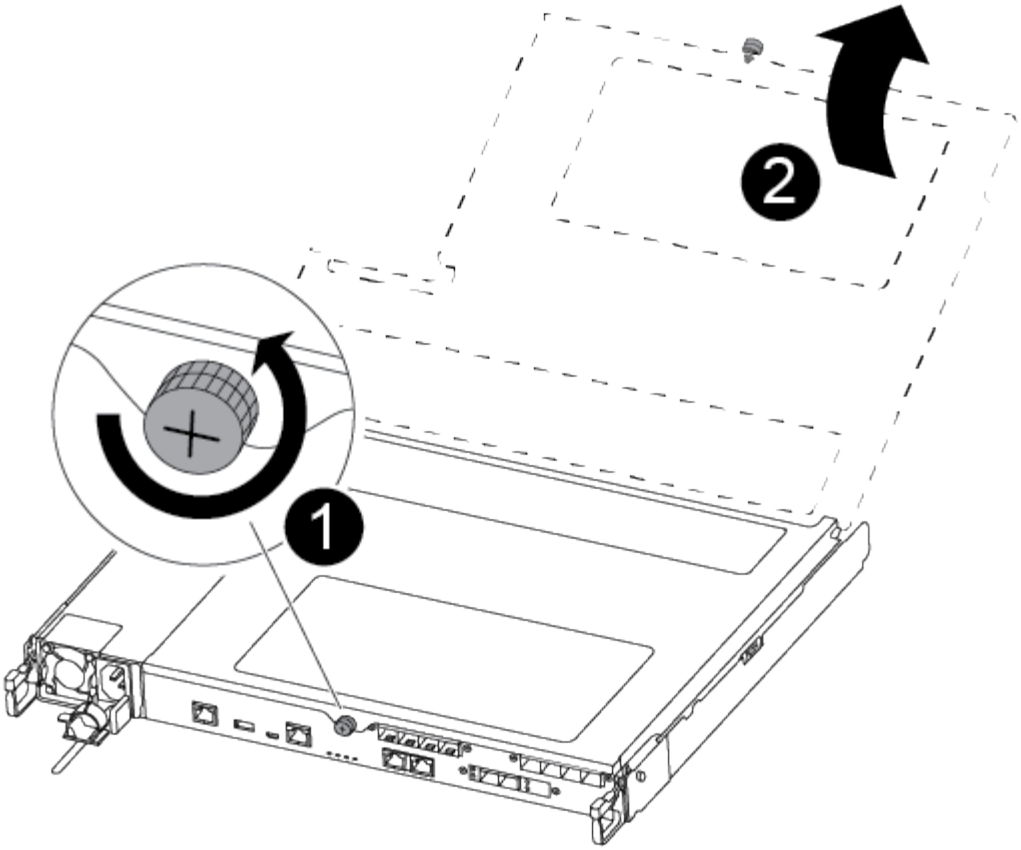
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



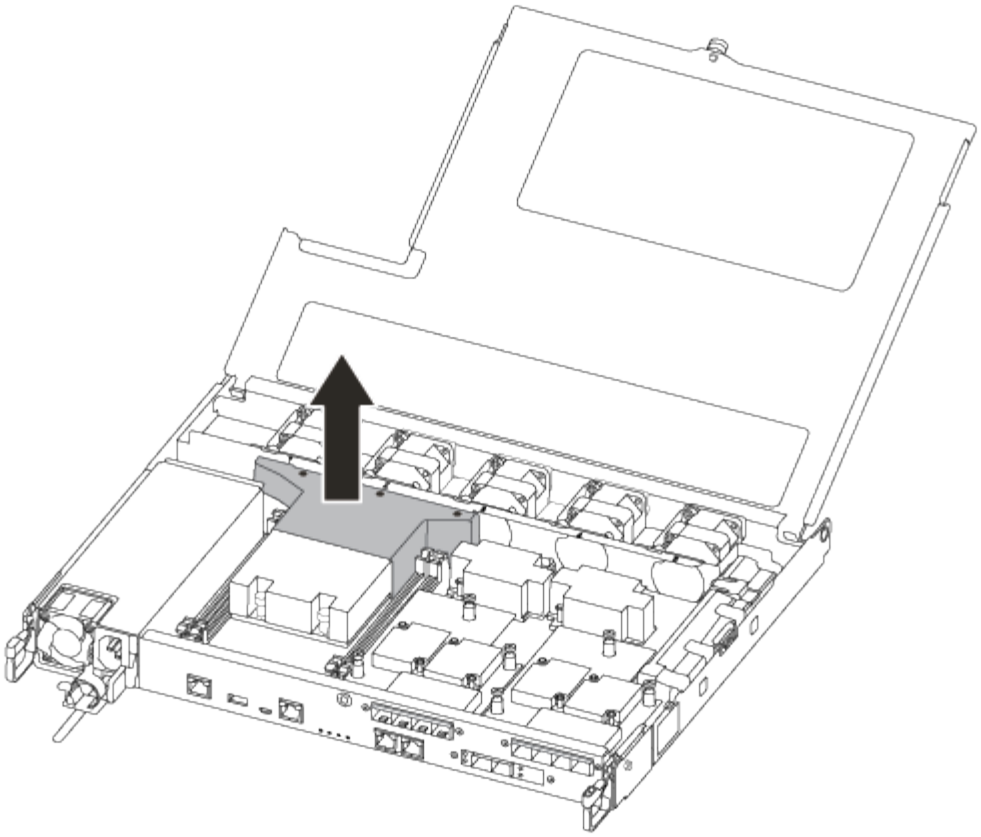
1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.



Step 2: Replace the boot media

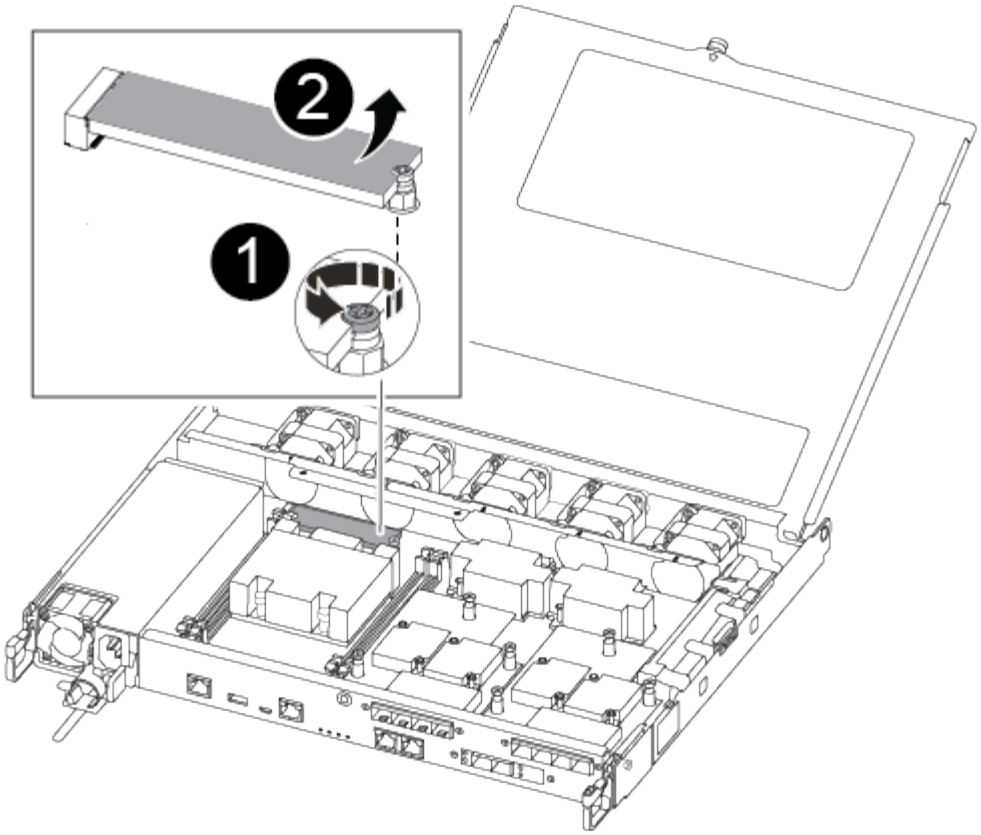
You locate the failed boot media in the controller module by removing the air duct on the controller module before you can replace the boot media.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not lose it.

You can use the following video or the tabulated steps to replace the boot media:

Animation - Replace the boot media

1. Locate and replace the impaired boot media from the controller module.



1	Remove the screw securing the boot media to the motherboard in the controller module.
2	Lift the boot media out of the controller module.

2. Using the #1 magnetic screwdriver, remove the screw from the impaired boot media, and set it aside safely on the magnet.
3. Gently lift the impaired boot media directly out of the socket and set it aside.
4. Remove the replacement boot media from the antistatic shipping bag and align it into place on the controller module.
5. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed is without a boot image so you need to transfer a boot image using a USB flash drive.

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download

button.

- If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.

- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
2. Download the service image to your work space on your laptop.
3. Unzip the service image.

   If you are extracting the contents using Windows, do not use winzip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

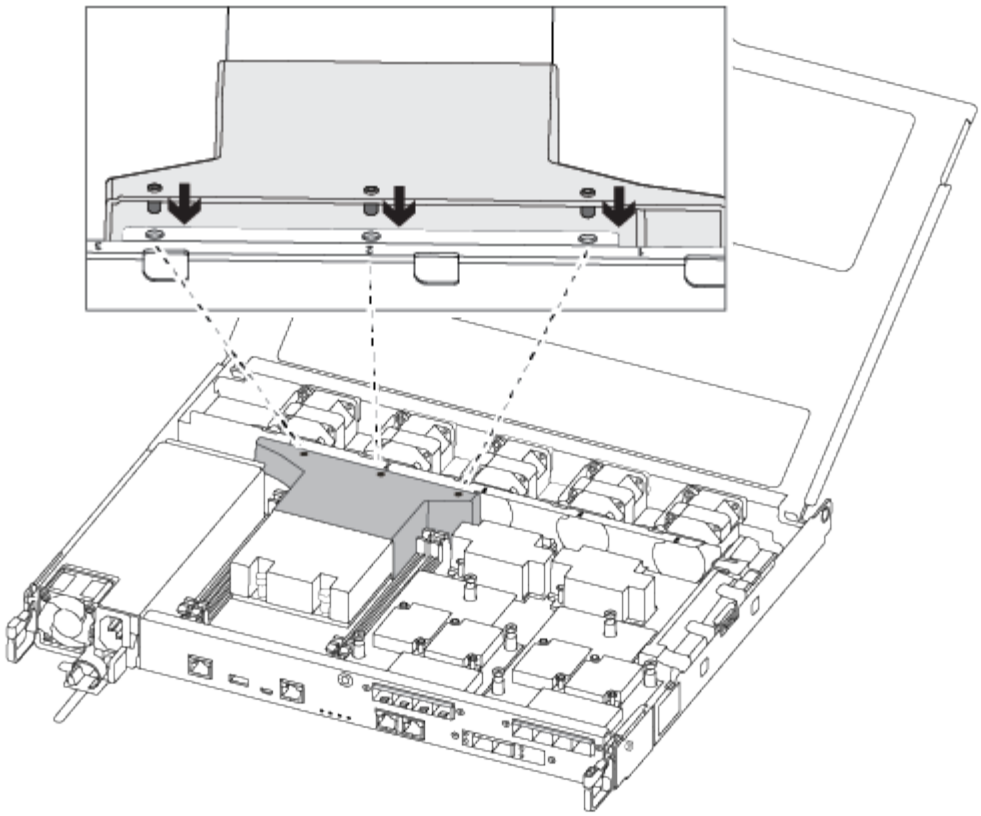
   There are two folders in the unzipped service image file:

   - boot
   - efi

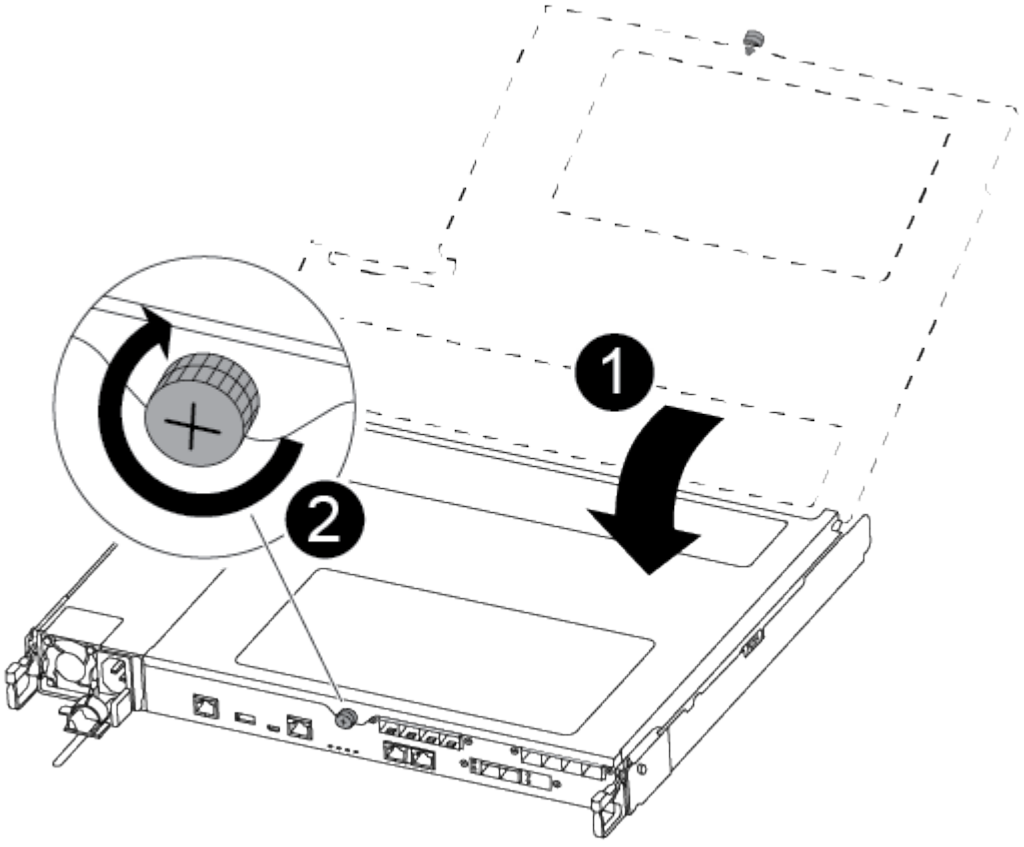
4. Copy the efi folder to the top directory on the USB flash drive.

   The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

5. Remove the USB flash drive from your laptop.
6. If you have not already done so, install the air duct.



7. Close the controller module cover and tighten the thumbscrew.



1	Controller module cover
2	Thumbscrew

8. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
9. Plug the power cable into the power supply and reinstall the power cable retainer.
10. Insert the USB flash drive into the USB slot on the controller module.

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

11. Push the controller module all the way into the chassis:
12. Place your index fingers through the finger holes from the inside of the latching mechanism.
13. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
14. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

    The controller module should be fully inserted and flush with the edges of the chassis.

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

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

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

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

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

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

    - If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
      - `filer_addr` is the IP address of the storage system.
      - `netmask` is the network mask of the management network that is connected to the HA partner.
      - `gateway` is the gateway for the network.

- `dns_addr` is the IP address of a name server on your network.
- `dns_domain` is the Domain Name System (DNS) domain name.

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

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

Boot the recovery image - ASA C250

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

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

   The image is downloaded from the USB flash drive.

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

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

If your system has…	Then…

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

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

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

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

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

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

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

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

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

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

   The image is downloaded from the USB flash drive.

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

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

If your system has…	Then…

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

4. Ensure that the environmental variables are set as expected:
   a. Take the controller to the LOADER prompt.
   b. Check the environment variable settings with the `printenv` command.
   c. If an environment variable is not set as expected, modify it with the `set` *`envenvironment_variable_name changed_value`* command.
   d. Save your changes using the `saveenv` command.
5. The next depends on your system configuration:

- If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed
- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

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

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

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

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

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

= Restore OKM, NSE, and NVE as needed - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

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

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

Steps

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

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

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

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

   Example of backup data:

   ```
   -----------------------BEGIN BACKUP-----------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1lWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   . . . .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

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

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

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local`

`-only-cfo-aggregates true` command.

- If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
- If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

  Terminating CIFS can cause loss of data.

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

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

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

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

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

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

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

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

    If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert -vserver Cluster -lif` *nodename* command.

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

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

Steps

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

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

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

     Terminating CIFS can cause loss of data.

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

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

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

  If the command fails, contact Customer Support.

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

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

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

= Return the failed part to NetApp - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

= Chassis

= Overview of chassis replacement - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

To replace the chassis, you must move the bezel, controller modules, and NVMe drives from the impaired chassis to the replacement chassis, and then remove the impaired chassis from the equipment rack or system cabinet and install the replacement chassis in its place.

About this task

- All other components in the system must be functioning properly; if not, you must contact technical support.
- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is written with the assumption that you are moving the bezel, NVMe drives, and controller modules to the new chassis, and that the replacement chassis is a new component from NetApp.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

= Shut down the controllers - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

This procedure is for 2-node, non-MetroCluster configurations only. If you have a system with more than two nodes, see How to perform a graceful shutdown and

power up of one HA pair in a 4-node cluster.

Before you begin

You need:

- Local administrator credentials for ONTAP.
- NetApp onboard key management (OKM) cluster-wide passphrase if using storage encryption.
- SP/BMC accessability for each controller.
- Stop all clients/host from accessing data on the NetApp system.
- Suspend external backup jobs.
- Necessary tools and equipment for the replacement.

If the system is a NetApp StorageGRID or ONTAP S3 used as FabricPool cloud tier, refer to the Gracefully shutdown and power up your storage system Resolution Guide after performing this procedure.

If using FlexArray array LUNs, follow the specific vendor storage array documentation for the shutdown procedure to perform for those systems after performing this procedure.

If using SSDs, refer to SU490: (Impact: Critical) SSD Best Practices: Avoid risk of drive failure and data loss if powered off for more than two months

As a best practice before shutdown, you should:

- Perform additional system health checks.
- Upgrade ONTAP to a recommended release for the system.
- Resolve any Active IQ Wellness Alerts and Risks. Make note of any faults presently on the system, such as LEDs on the system components.

Steps

1. Log into the cluster through SSH or log in from any node in the cluster using a local console cable and a laptop/console.
2. Turn off AutoSupport and indicate how long you expect the system to be off line:

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

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

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

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

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

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

6. Halt all nodes in the cluster:

```
system node halt -node * -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 * -skip-lif-migration-before-shutdown true -ignore-quorum-warnings true -inhibit-takeover true -ignore -strict-sync-warnings true`

7. Enter **y** for each controller in the cluster when you see *`Warning: Are you sure you want to halt node "cluster name-controller number"? {y|n}:`*
8. Wait for each controller to halt and display the LOADER prompt.
9. Turn off each PSU or unplug them if there is no PSU on/off switch.
10. Unplug the power cord from each PSU.
11. Verify that all controllers in the impaired chassis are powered down.

= Replace hardware - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

To replace the chassis, you move the power supplies, hard drives, and controller module from the impaired chassis to the new chassis, and swap out the impaired chassis from with the new chassis of the same model as the impaired chassis.

== Step 1: Remove the controller modules

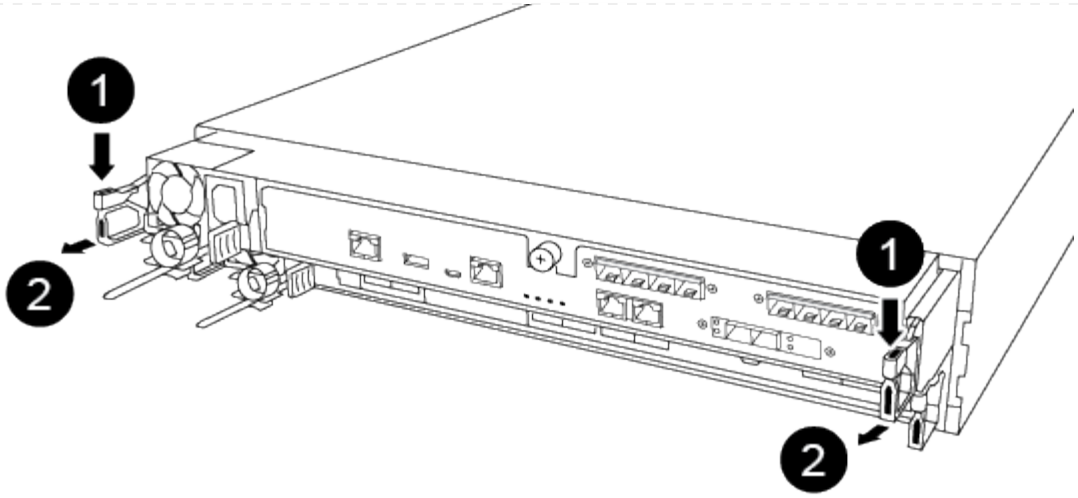
To replace the chassis, you must remove the controller modules from the old chassis.

Use the following video or the tabulated steps to replace the chassis; it assumes the removal and replacement of the bezel:

Animation - Replace the chassis

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

== Step 2: Move drives to the new chassis

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

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

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

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

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

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

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

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

== Step 3: Replace a chassis from within the equipment rack or system cabinet

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

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

== Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot the system.

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

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

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

2. Recable the console to the controller module, and then reconnect the management port.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

The controller module should be fully inserted and flush with the edges of the chassis.

5. Repeat the preceding steps to install the second controller into the new chassis.

= Complete the restoration and replacement process - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

You must verify the HA state of the chassis, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

== Step 1: Verify and set the HA state of the chassis

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

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

   The HA state should be the same for all components.

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

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

      - `ha`
      - `mcc`
      - `mccip`
      - `non-ha`

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

== Step 2: Return the failed part to NetApp

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

= Controller

= Overview of controller module replacement- ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

- All drive shelves must be working properly.
- If your system is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.

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

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

= Shut down the impaired controller module - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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 impaired controller SCSI blade. The `cluster kernel-service show` command 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=number_of_hours_downh`

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

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`

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

3. Take the impaired controller to the LOADER prompt:

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

= Replace the controller module hardware - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

== Step 1: Remove the controller module

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

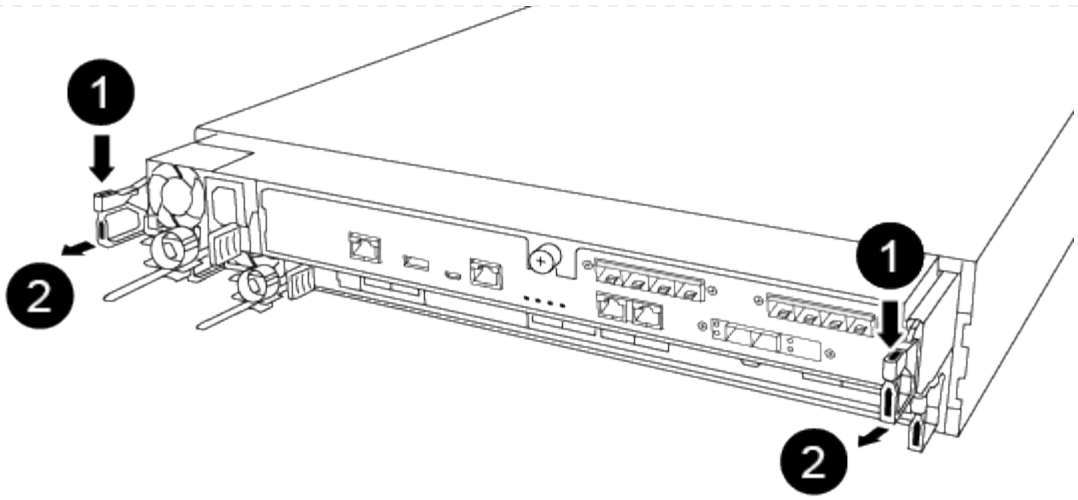
Make sure that you label the cables so that you know where they came from.

Use the following video or the tabulated steps to replace a controller module:

Animation - Replace a controller module

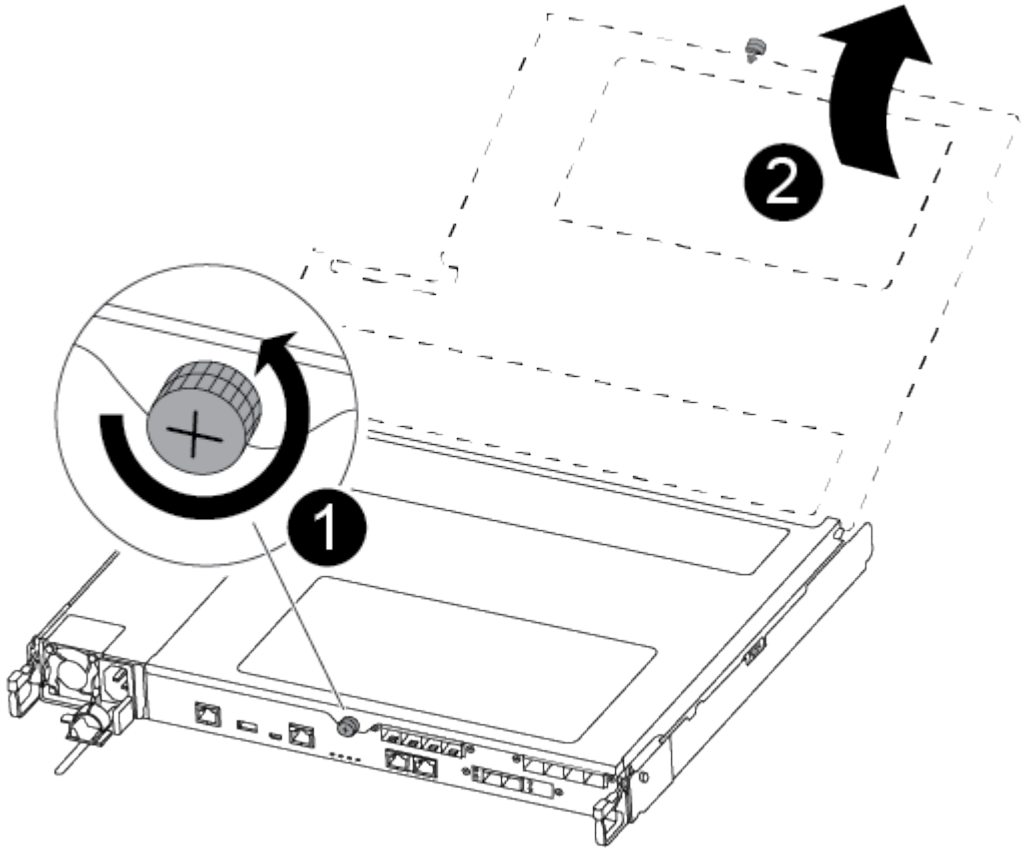
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



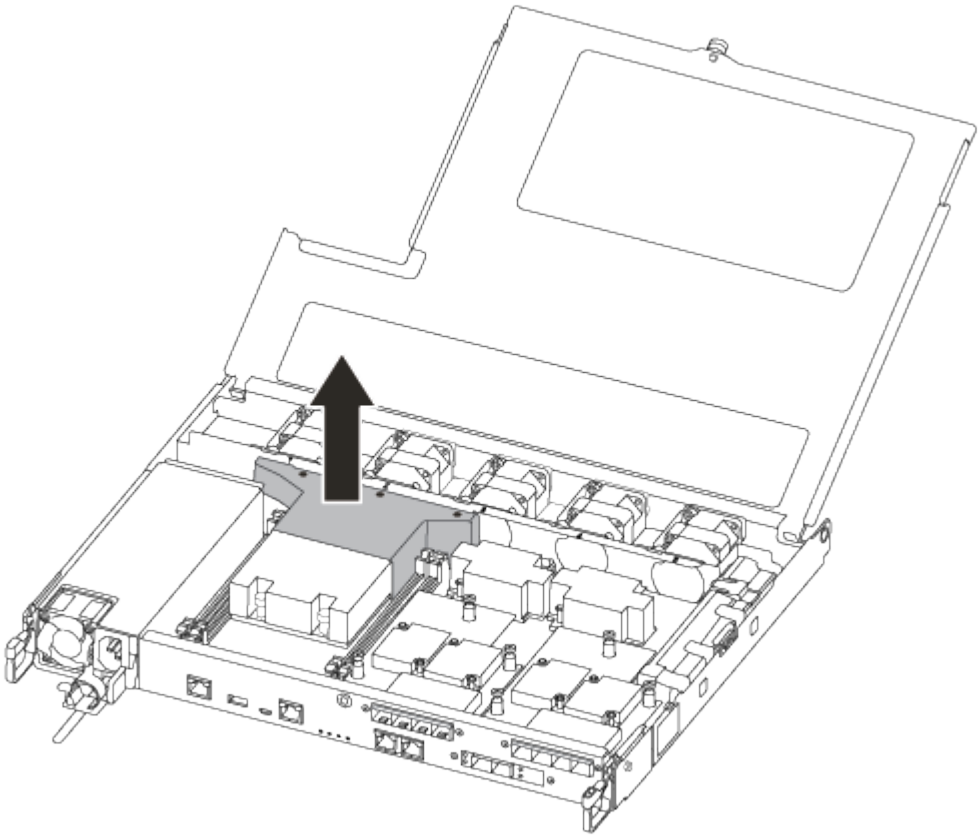
1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.



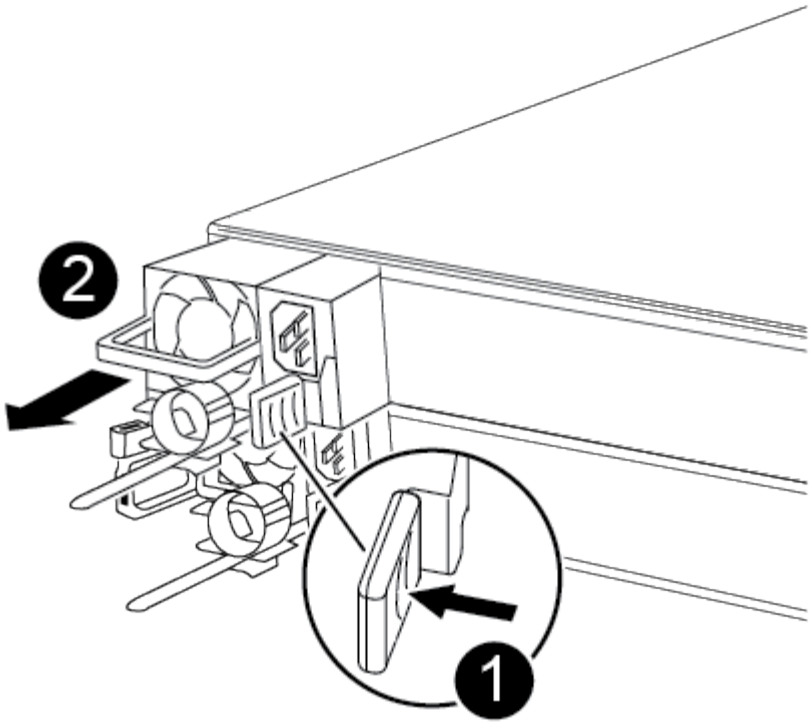
== Step 2: Move the power supply

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

1. Disconnect the power supply.
2. Open the power cable retainer, and then unplug the power cable from the power supply.
3. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

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

The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.



1	Blue power supply locking tab
2	Power supply

5. Move the power supply to the new controller module, and then install it.
6. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

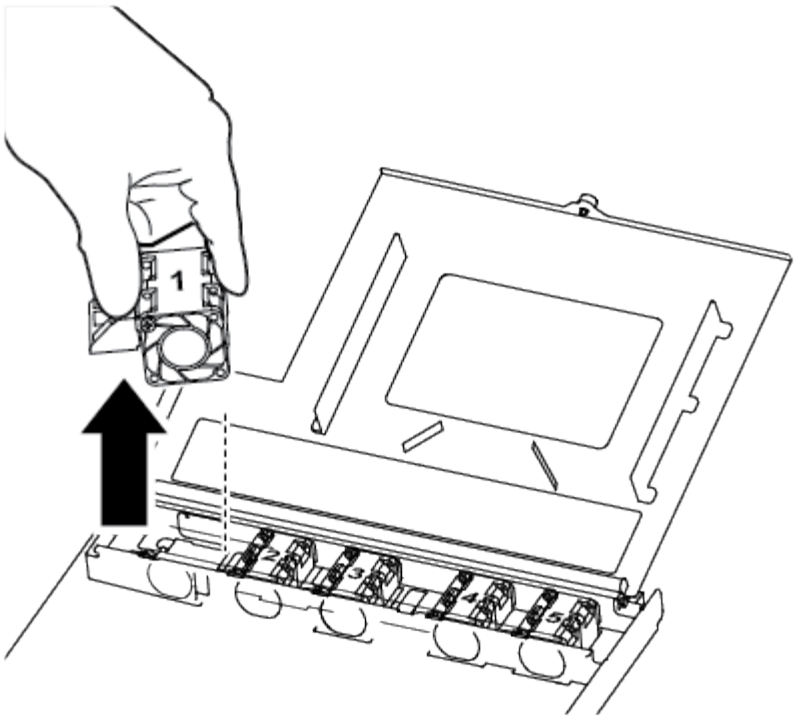
   The power supplies will only properly engage with the internal connector and lock in place one way.

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

== Step 3: Move the fans

You must move the fans from the impaired controller module to the replacement module when replacing a failed controller module.

1. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.



1	Fan module

2. Move the fan module to the replacement controller module, and align the edges of the fan module with the opening in the controller module, and then slide the fan module in.
3. Repeat these steps for the remaining fan modules.

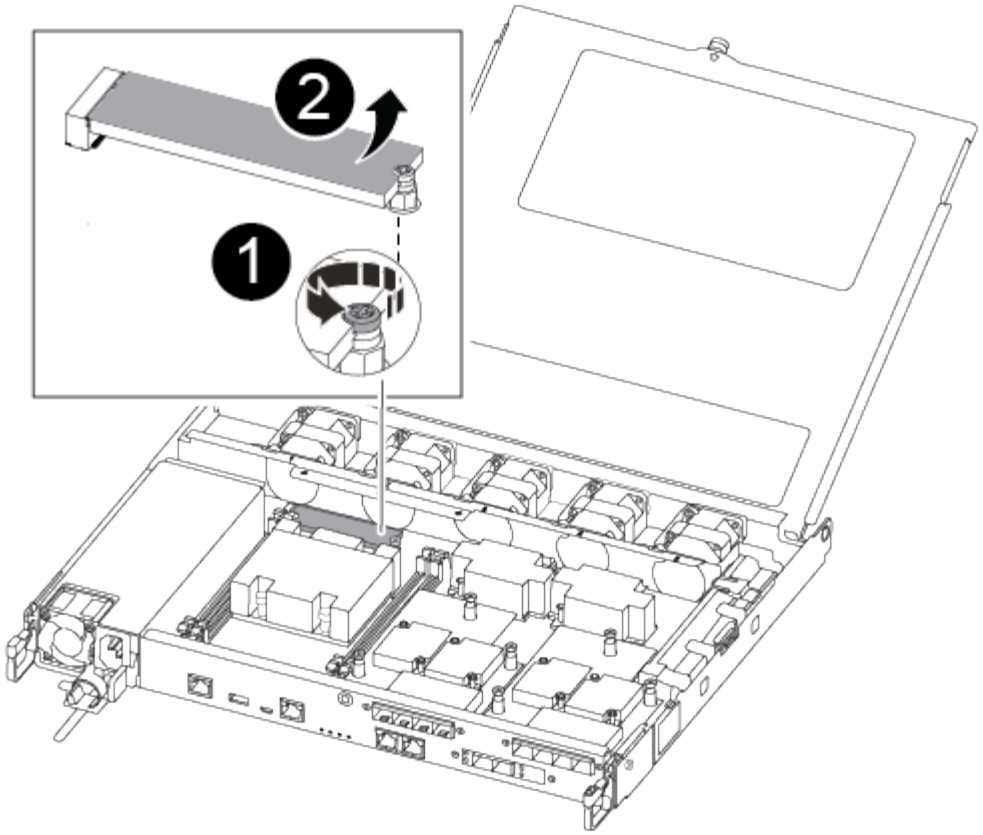
== Step 4: Move the boot media

You must move the boot media device from the impaired controller module to the replacement controller module.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not lose it.

1. Locate and move the boot media from the impaired controller module to the replacement controller module.

   The boot media is located under the air duct cover you removed earlier in this procedure.



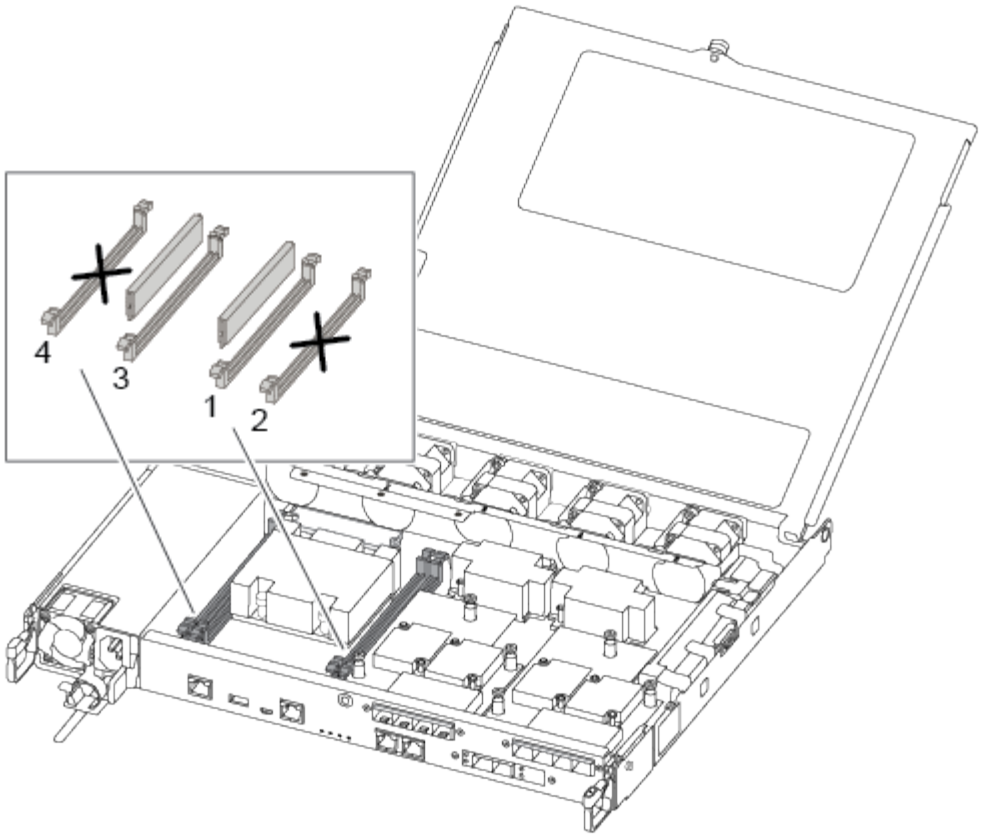
1	Remove the screw securing the boot media to the motherboard in the impaired controller module.
2	Lift the boot media out of the impaired controller module.

2. Using the #1 magnetic screwdriver, remove the screw from the boot media, and set it aside safely on the magnet.
3. Gently lift the boot media directly out of the socket and align it into place in the replacement controller module.
4. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

== Step 5: Move the DIMMs

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



Install each DIMM into the same slot it occupied in the impaired controller module.

1. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.

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

2. Locate the corresponding DIMM slot on the replacement controller module.
3. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

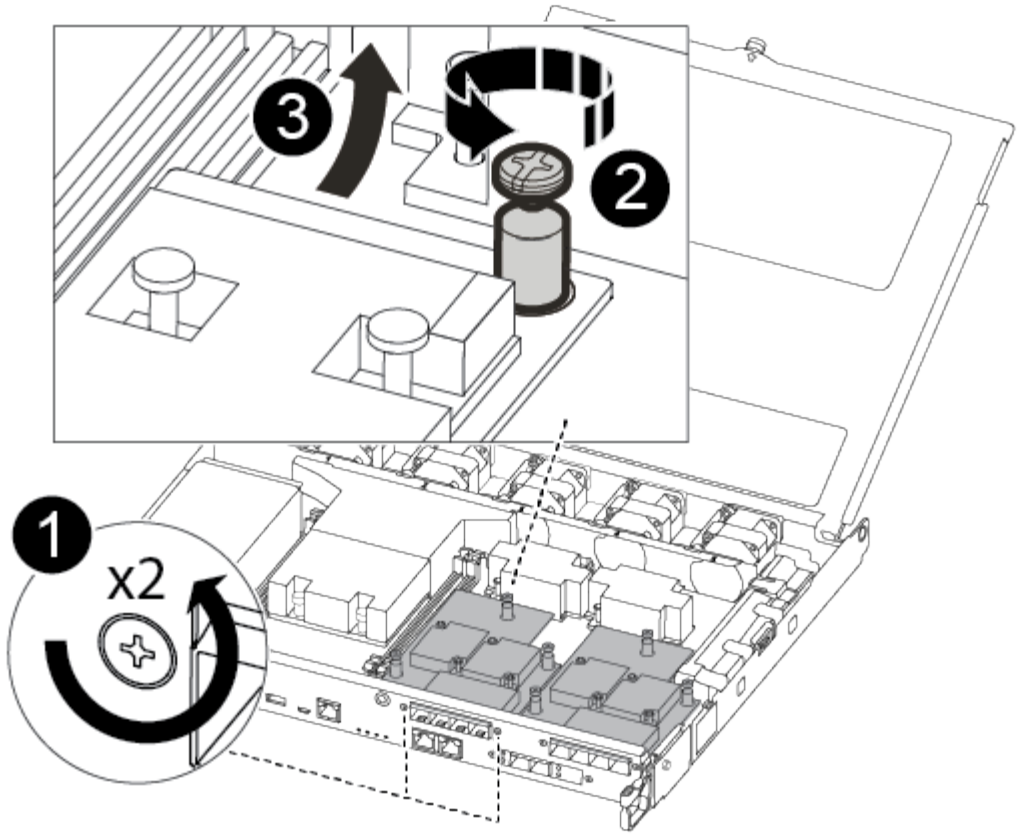
   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

4. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
5. Repeat these steps for the remaining DIMM.

== Step 6: Move a mezzanine card

To move a mezzanine card, you must remove the cabling and any QSFPs and SFPs from the ports, move the mezzanine card to the replacement controller, reinstall any QSFPs and SFPs onto the ports, and cable the ports.

1. Locate and move the mezzanine cards from your impaired controller module.



1	Remove screws on the face of the controller module.
2	Loosen the screw in the controller module.
3	Move the mezzanine card.

2. Unplug any cabling associated with the mezzanine card.

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

   a. Remove any SFP or QSFP modules that might be in the mezzanine card and set it aside.
   b. Using the #1 magnetic screwdriver, remove the screws from the face of the impaired controller module and from the mezzanine card, and set them aside safely on the magnet.
   c. Gently lift the mezzanine card out of the socket and move it to the same position in the replacement controller.
   d. Gently align the mezzanine card into place in the replacement controller.
   e. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the replacement controller module and on the mezzanine card.

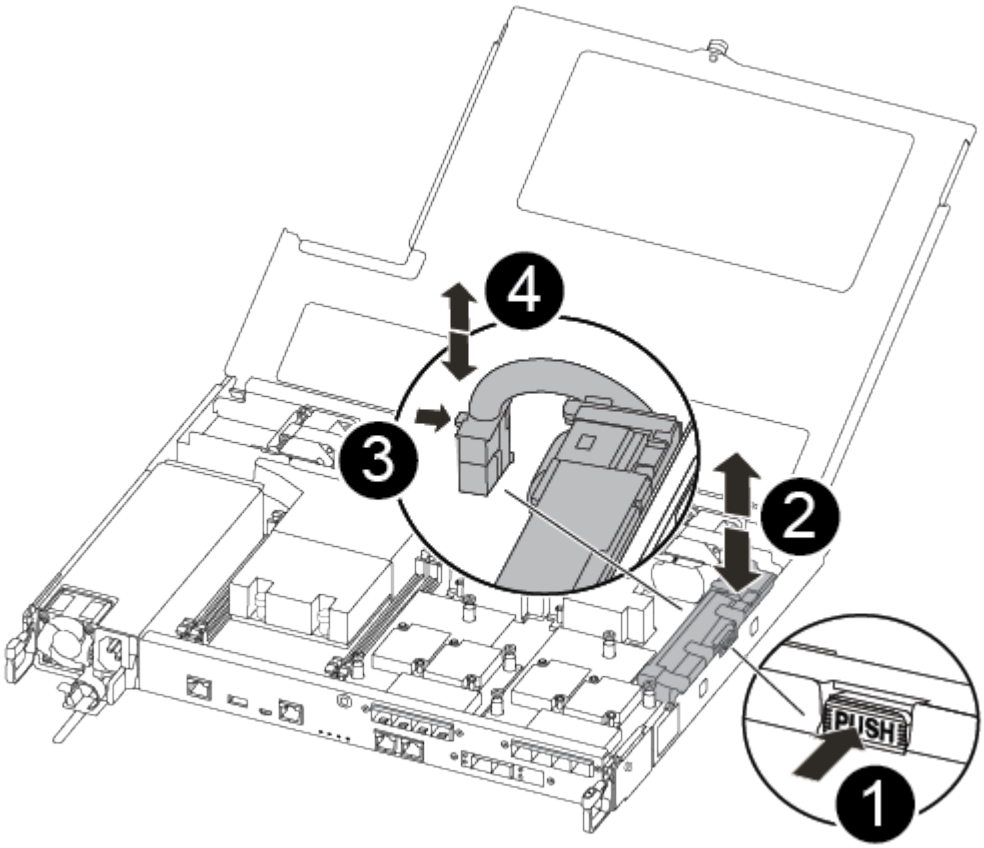
   > Do not apply force when tightening the screw on the mezzanine card; you might crack it.

3. Repeat these steps if there is another mezzanine card in the impaired controller module.
4. Insert the SFP or QSFP modules that were removed onto the mezzanine card.

== Step 7: Move the NV battery

When replacing the controller module, you must move the NV battery from the impaired controller module to the replacement controller module.

1. Locate and move the NVMEM battery from your impaired controller module to the replacement controller module.



1	Squeeze the clip on the face of the battery plug.
2	Unplug the battery cable from the socket.
3	Grasp the battery and press the blue locking tab marked PUSH.
4	Lift the battery out of the holder and controller module.

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.

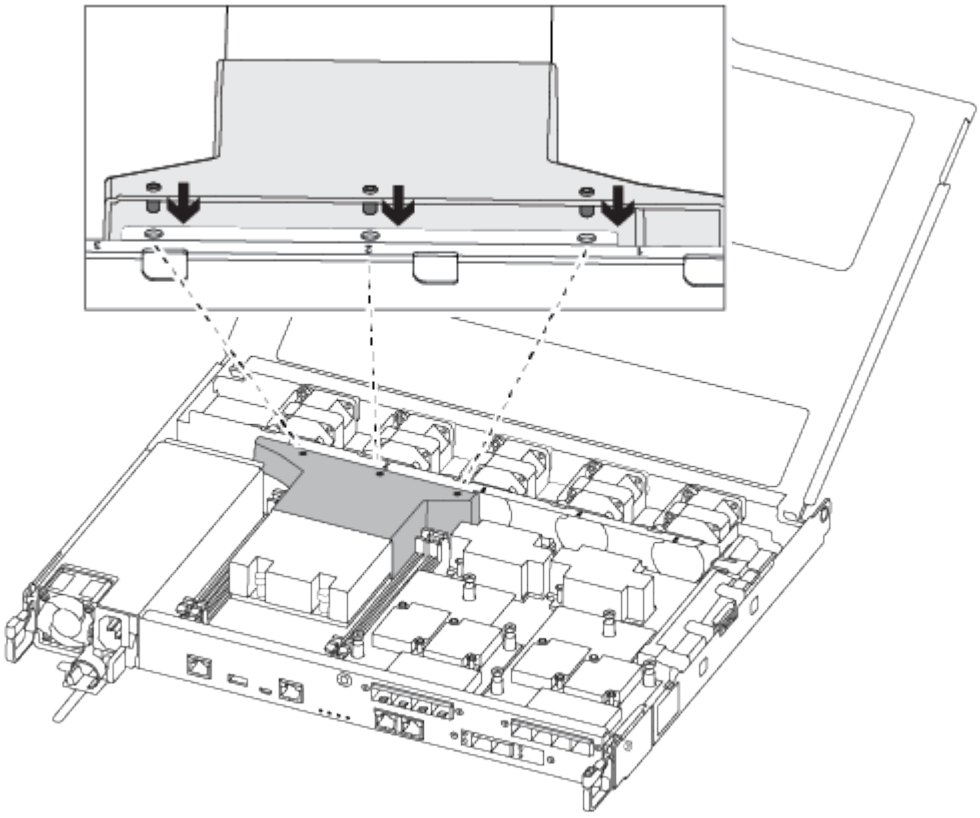
4. Locate the corresponding NV battery holder on the replacement controller module and align the NV battery to the battery holder.
5. Insert the NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

== Step 8: Install the controller module

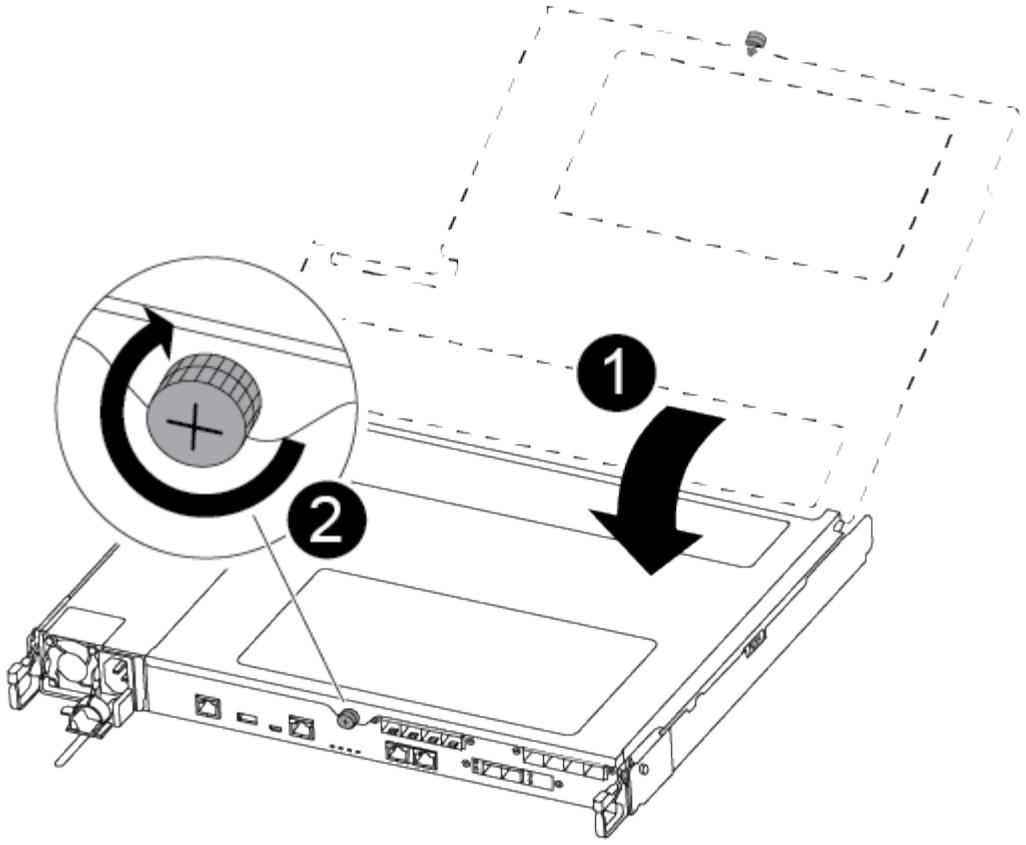
After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustrations or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.



2. Close the controller module cover and tighten the thumbscrew.



1	Controller module cover
2	Thumbscrew

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

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

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

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

5. Insert the controller module into the chassis:
6. Ensure the latching mechanism arms are locked in the fully extended position.
7. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
8. Place your index fingers through the finger holes from the inside of the latching mechanism.
9. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
10. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching

mechanisms snap into place.

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

The controller module should be fully inserted and flush with the edges of the chassis.

= Restore and verify the system configuration - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

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

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

About this task

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

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

Steps

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

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

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

The HA state should be the same for all components.

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

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

   - ha
   - mcc
   - mccip
   - non-ha

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

= Recable the system and reassign disks - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

== Step 1: Recable the system

Recable the controller module's storage and network connections.

Steps

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

== Step 2: Reassign disks

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

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

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

console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

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

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

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

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

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

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

   d. Return to the admin privilege level: `set -privilege admin`
5. If your storage system has Storage or Volume Encryption configured, you must restore Storage or Volume Encryption functionality by using one of the following procedures, depending on whether you are using onboard or external key management:
   - Restore onboard key management encryption keys
   - Restore external key management encryption keys
6. Give back the controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

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

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

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

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

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

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

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

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

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

Disk  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
.
.
.
```

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

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

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

This is required if both of the following are true:

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

Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

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

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

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

4 entries were displayed.
```

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

= Complete system restoration - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

== Step 1: Install licenses for the replacement controller in ONTAP

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

About this task

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

Before you begin

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

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

Steps

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

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

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

== Step 2: Verify LIFs and registering the serial number

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

Steps

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

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

2. Register the system serial number with NetApp Support.
   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.
3. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.
4. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

== Step 3: Return the failed part to NetApp

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

= Replace a DIMM - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

About this task

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

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

== Step 1: Shut down the impaired controller

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for impaired controller SCSI blade. The `cluster kernel-service show` command 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=number_of_hours_downh`

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

== Step 2: Remove the controller module

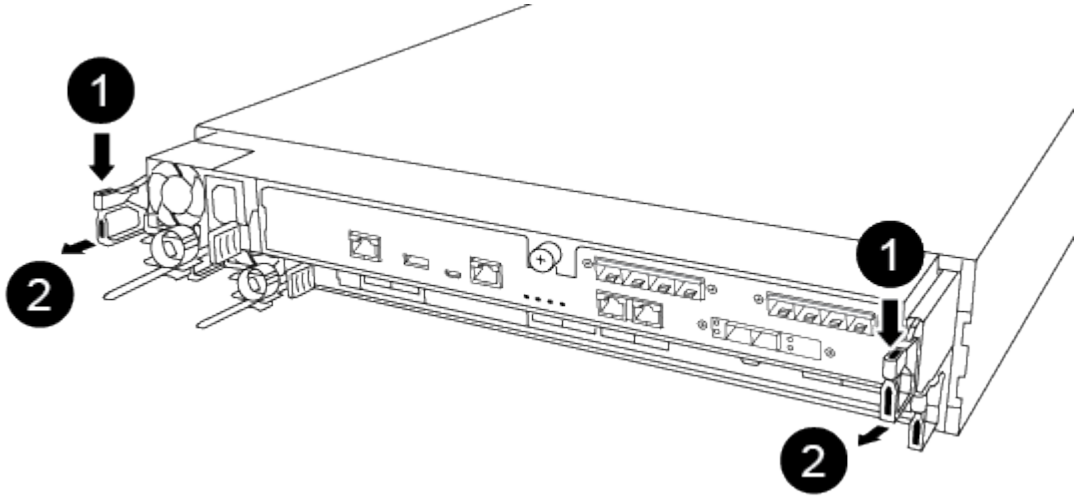
You must remove the controller module from the chassis when you replace a component inside the

controller module.

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

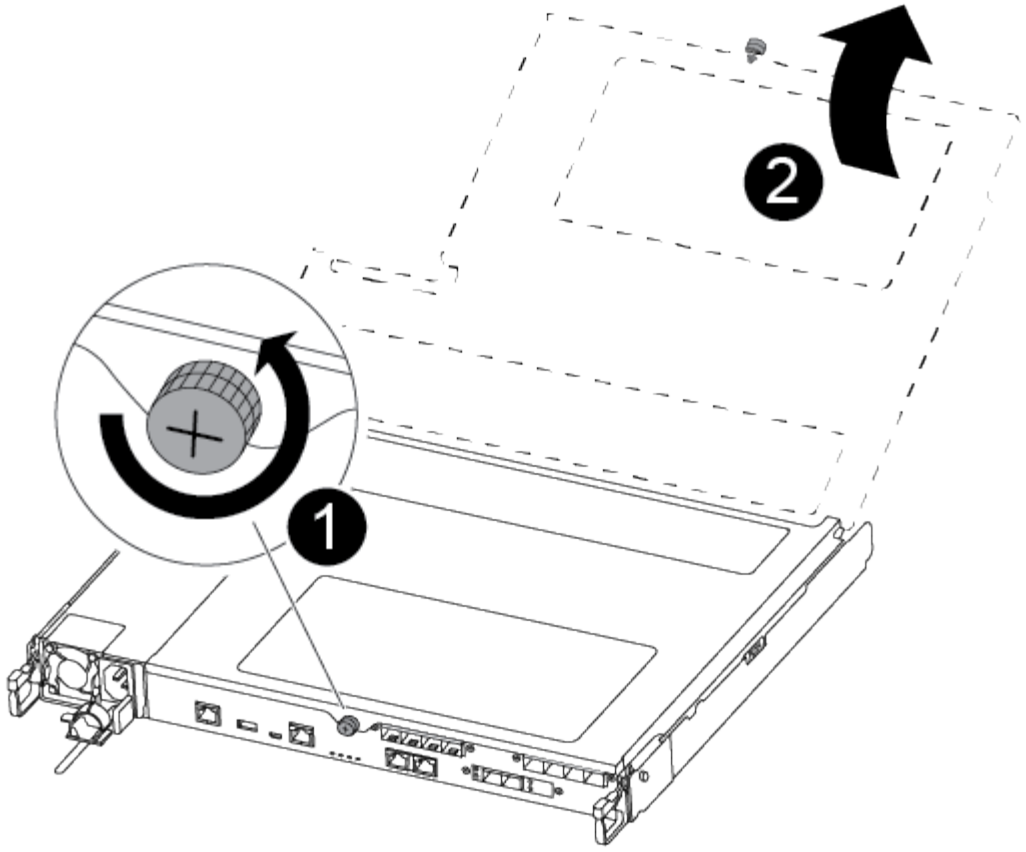
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



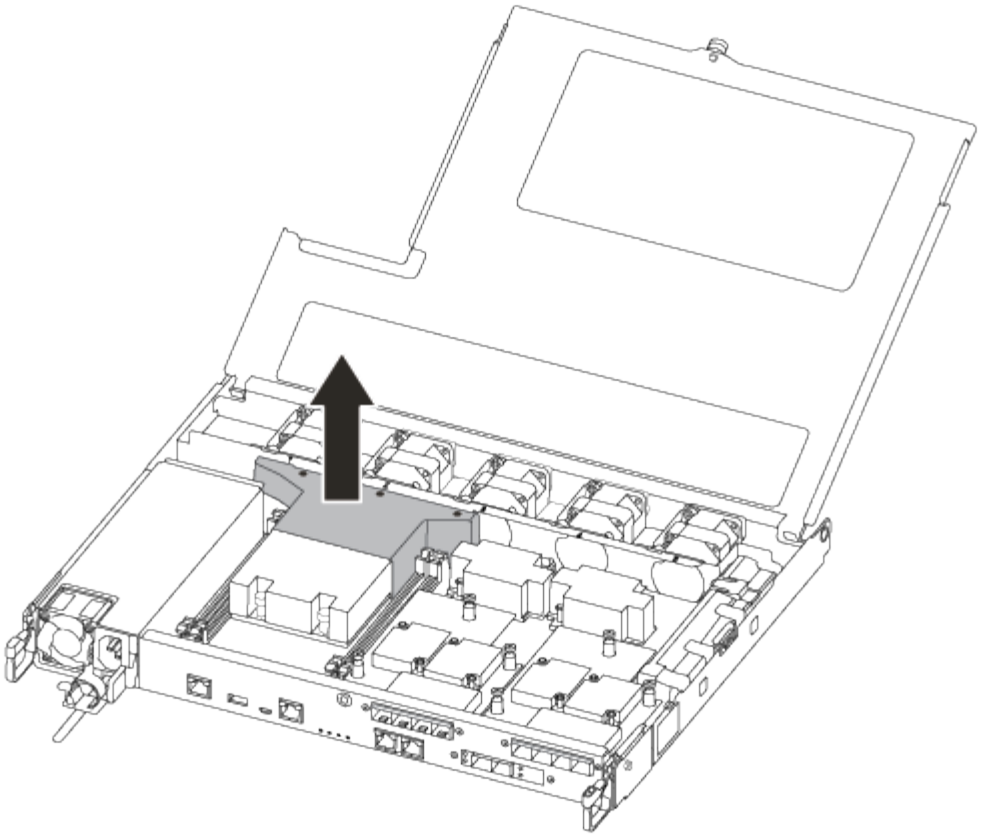
1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.



== Step 3: Replace a DIMM

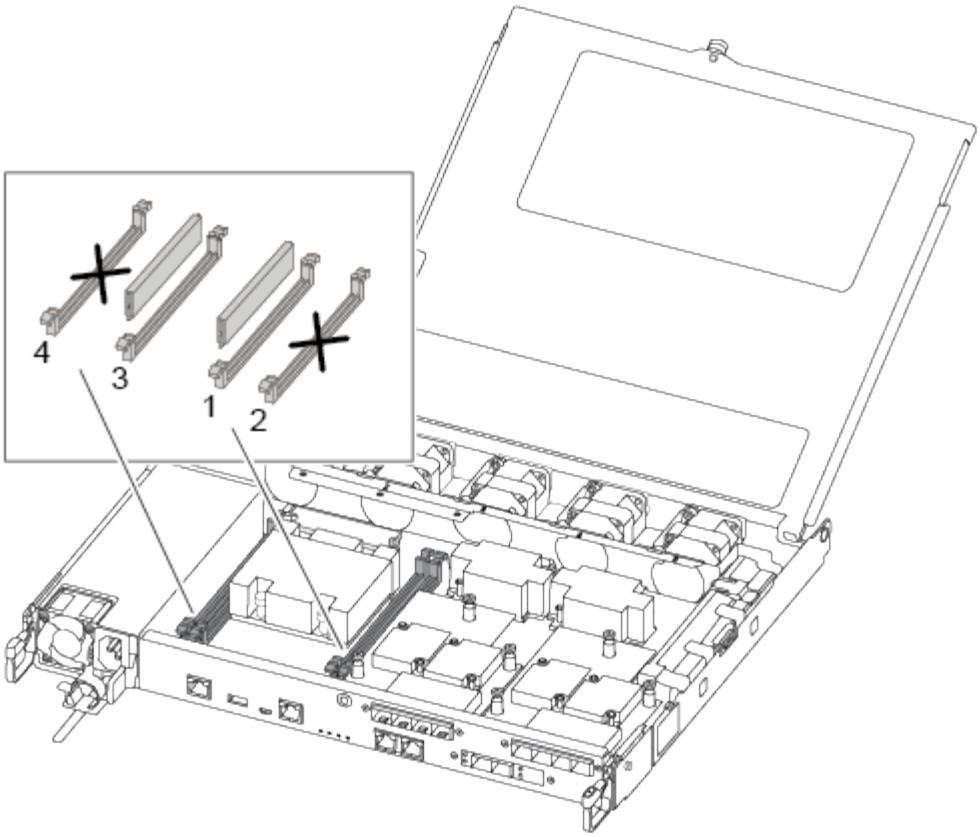
To replace a DIMM, you must locate it in the controller module using the DIMM map label on top of the air duct and then replace it following the specific sequence of steps.

Use the following video or the tabulated steps to replace a DIMM:

Animation - Replace a DIMM

1. Replace the impaired DIMM on your controller module.

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



2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
3. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.
4. Leave DIMM ejector tabs on the connector in the open position.
5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

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

6. Insert the replacement DIMM squarely into the slot.

   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

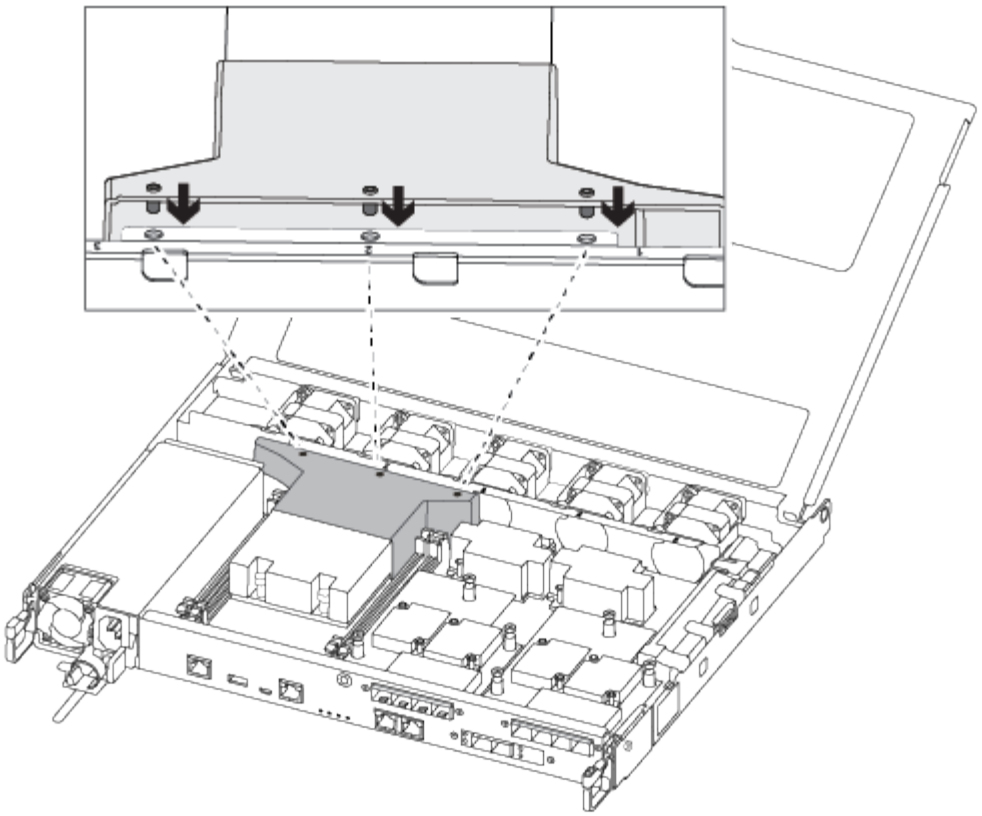
7. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.

== Step 4: Install the controller module

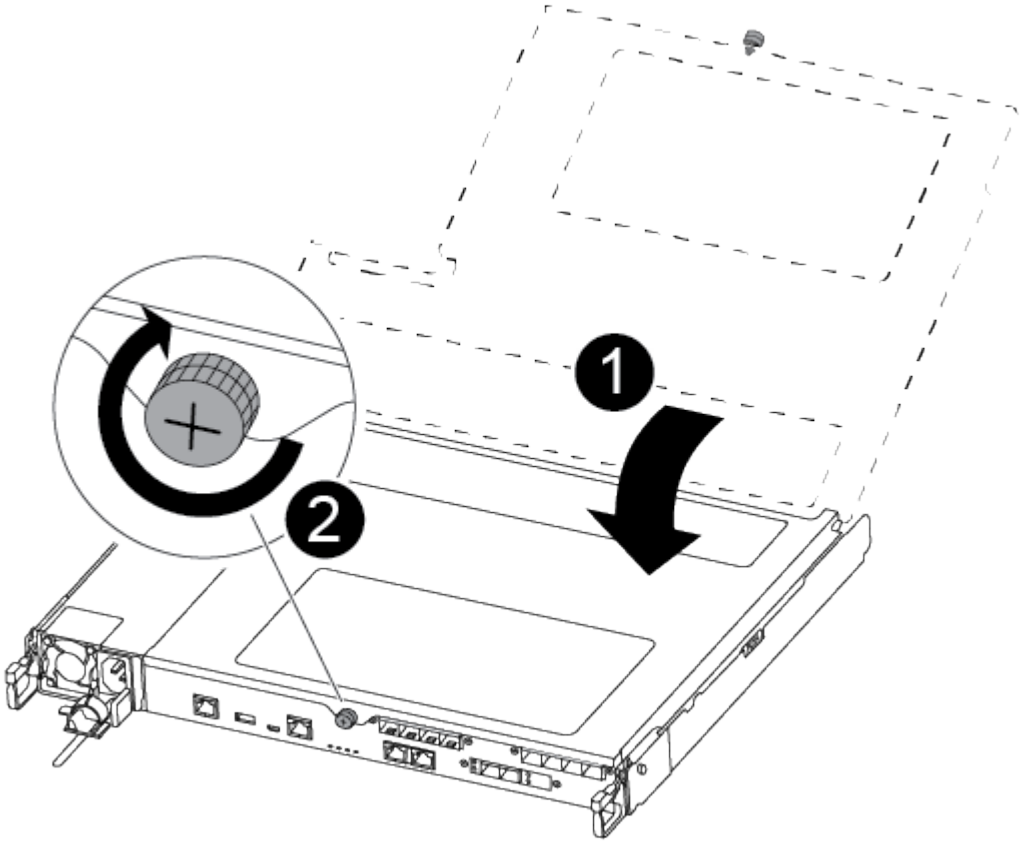
After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it.

You can use the following illustrations or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.



2. Close the controller module cover and tighten the thumbscrew.



1	Controller module cover
2	Thumbscrew

3. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

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

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

== Step 5: Return the failed part to NetApp

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

= Replace SSD Drive or HDD Drive - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

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

Before you begin

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

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

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

- Determine whether SED authentication is enabled.

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

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

About this task

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

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

Procedure

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

Option 1: Replace SSD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.

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

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

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

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

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

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

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

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

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

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

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

      You can enter the command on either controller module.

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

      You can enter the command on either controller module.

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

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

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

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

Option 2: Replace HDD

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

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

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

      You can enter the command on either controller module.

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

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

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

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

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

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

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

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

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

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

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

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

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

       You can enter the command on either controller module.

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

       You can enter the command on either controller module.

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

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

       You must reenable automatic drive assignment on both controller modules.

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

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

= Replace a fan - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

To replace a fan, remove the failed fan module and replace it with a new fan module.

== Step 1: Shut down the impaired controller

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for impaired controller SCSI blade. The `cluster kernel-service show` command 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=number_of_hours_downh`

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.

If the impaired controller is displaying…	Then…
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` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

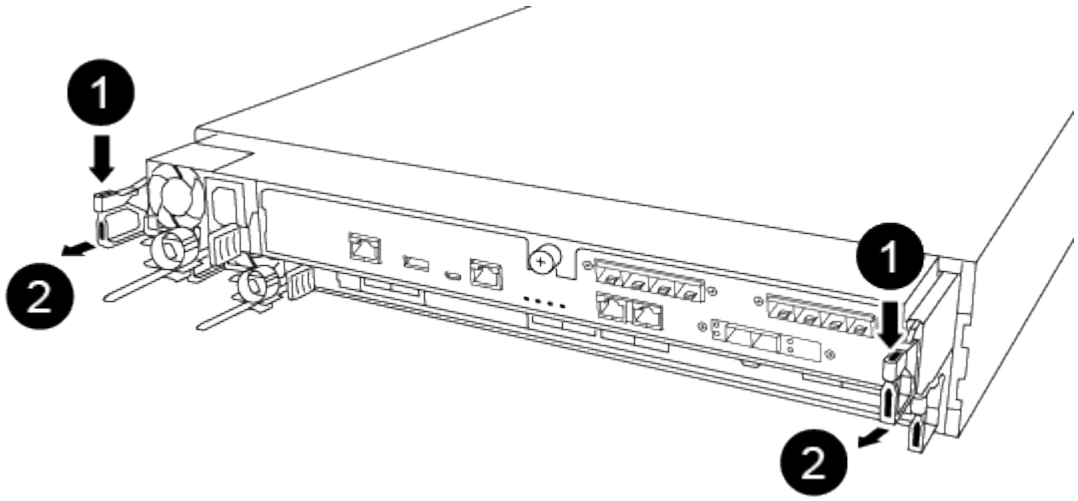
== Step 2: Remove the controller module

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

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

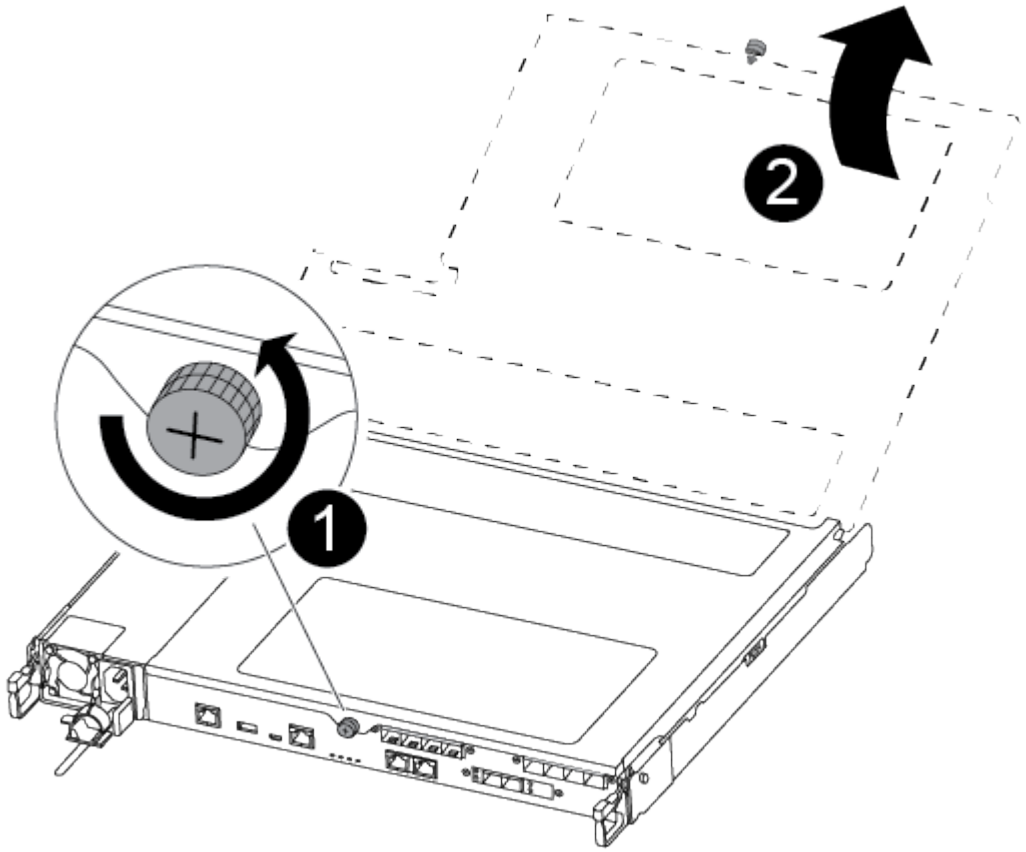
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover

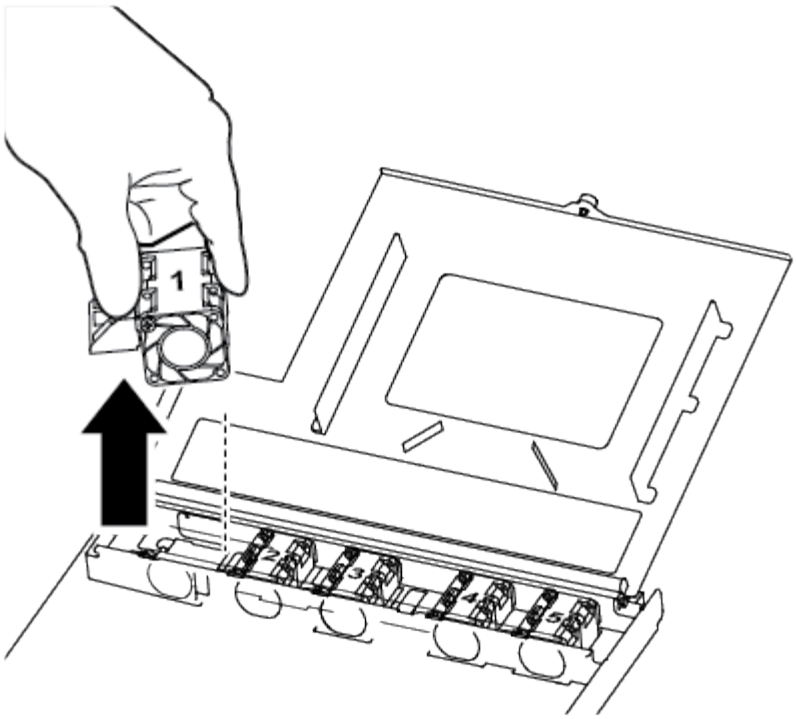
== Step 3: Replace a fan

To replace a fan, remove the failed fan module and replace it with a new fan module.

Use the following video or the tabulated steps to replace a fan:

Animation - Replace a fan

1. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
2. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.



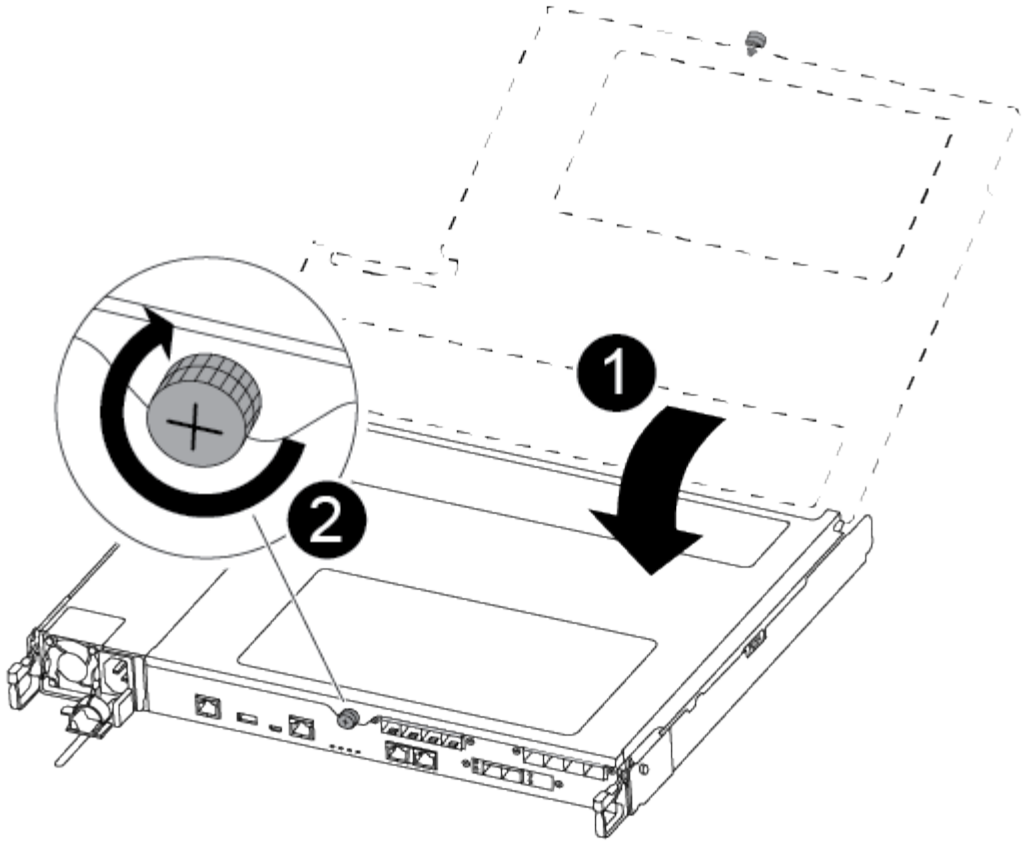
1	Fan module

3. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module.

== Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.



1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

== Step 5: Return the failed part to NetApp

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

= Replace or install a mezzanine card - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

To replace a failed mezzanine card, you must remove the cables and any SFP or QSFP modules, replace the card, reinstall the SFP or QSFP modules and recable the cards. To install a new mezzanine card, you must have the appropriate cables and SFP or QSFP modules.

About this task

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

== Step 1: Shut down the impaired controller

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 impaired controller SCSI blade. The `cluster kernel-service show` command 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=number_of_hours_downh`

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

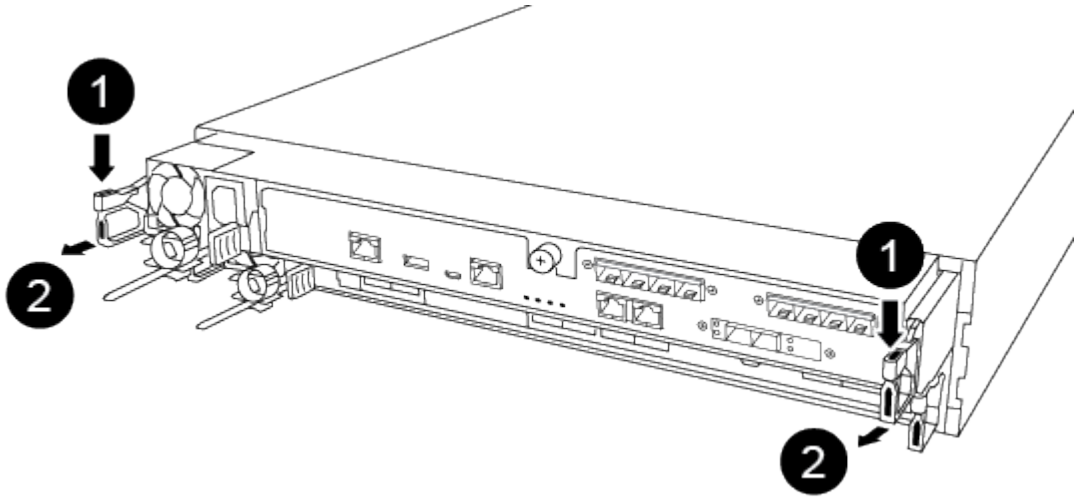
== Step 2: Remove the controller module

Remove the controller module from the chassis when you replace a component inside the controller module.

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

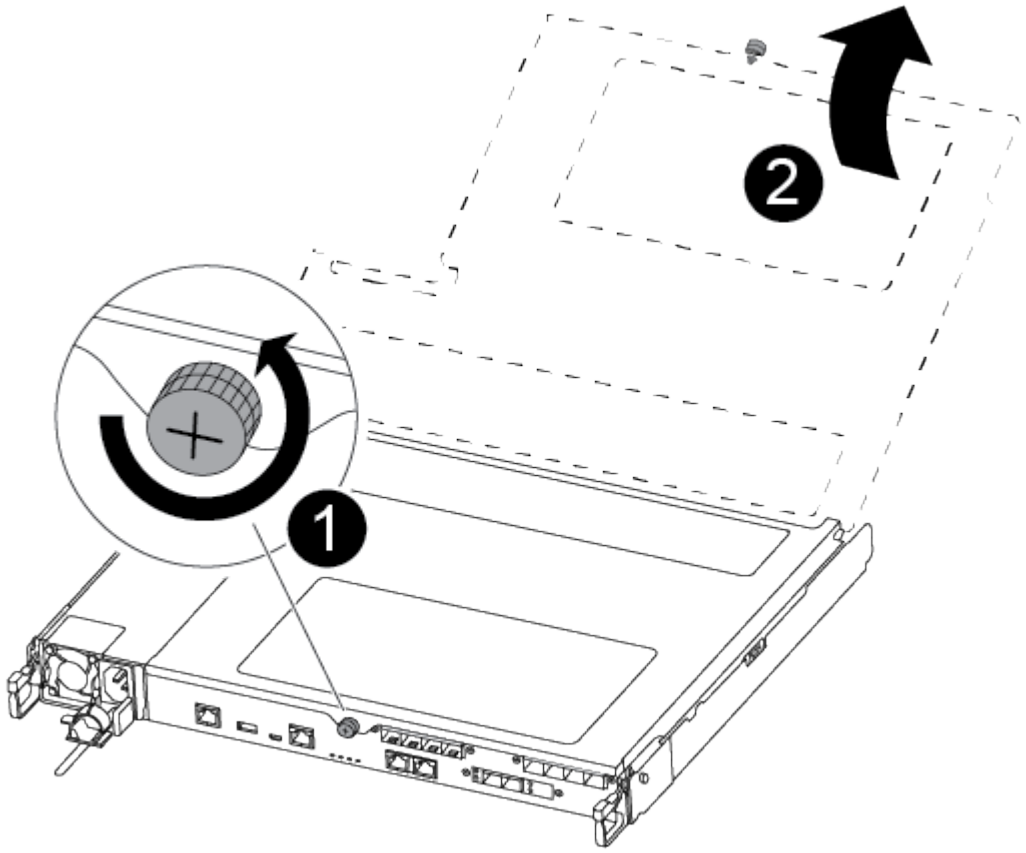
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover.

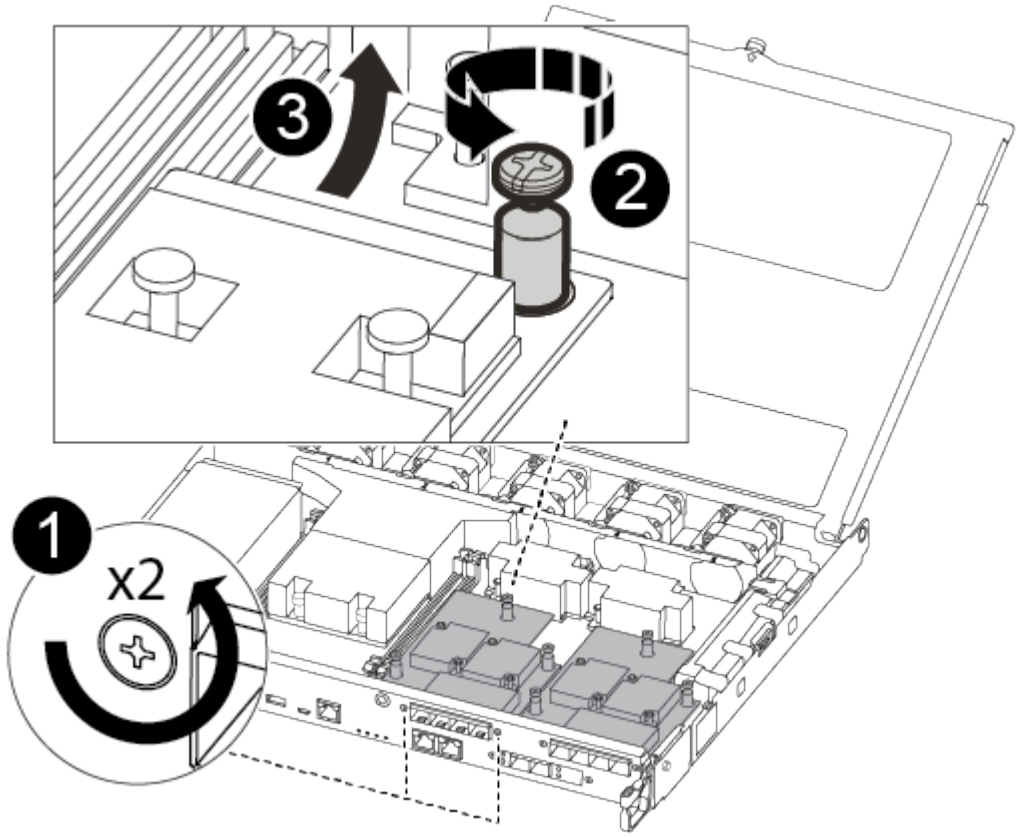
== Step 3: Replace or install a mezzanine card

To replace a mezzanine card, you must remove the impaired card and install the replacement card; to install a mezzanine card, you must remove the faceplate and install the new card.

Use the following video or the tabulated steps to replace a mezzanine card:

Animation - Replace a mezzanine card

1. To replace a mezzanine card:
2. Locate and replace the impaired mezzanine card on your controller module.



1	Remove screws on the face of the controller module.
2	Loosen the screw in the controller module.
3	Remove the mezzanine card.

a. Unplug any cabling associated with the impaired mezzanine card.

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

b. Remove any SFP or QSFP modules that might be in the impaired mezzanine card and set it aside.

c. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and set them aside safely on the magnet.

d. Using the #1 magnetic screwdriver, loosen the screw on the impaired mezzanine card.

e. Using the #1 magnetic screwdriver, gently lift the impaired mezzanine card directly out of the socket and set it aside.

f. Remove the replacement mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.

g. Gently align the replacement mezzanine card into place.

h. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

> Do not apply force when tightening the screw on the mezzanine card; you might crack it.

i. Insert any SFP or QSFP modules that were removed from the impaired mezzanine card to the replacement mezzanine card.

3. To install a mezzanine card:
4. You install a new mezzanine card if your system does not have one.

a. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and the faceplate covering the mezzanine card slot, and set them aside safely on the magnet.

b. Remove the mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.

c. Gently align the mezzanine card into place.

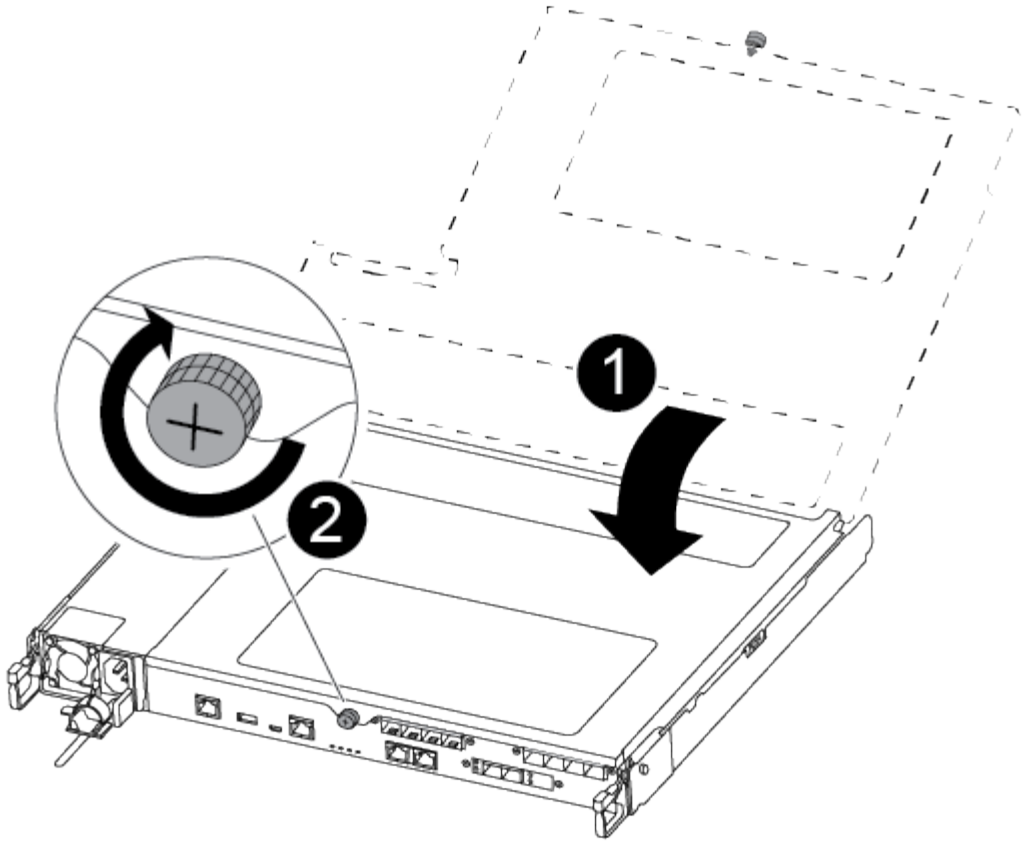
d. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

> Do not apply force when tightening the screw on the mezzanine card; you might crack it.

== Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.



1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

== Step 5: Return the failed part to NetApp

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

= Replace the NVMEM battery - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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

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

== Step 1: Shut down the impaired controller

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for impaired controller SCSI blade. The `cluster kernel-service show` command 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=number_of_hours_downh`

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

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify –node local -auto-giveback false`

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

3. Take the impaired controller to the LOADER prompt:

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

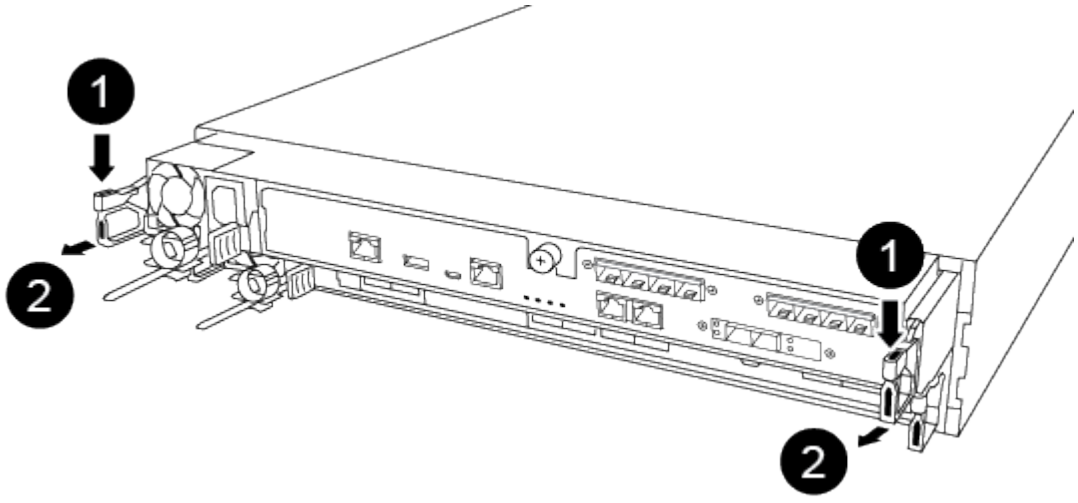
== Step 2: Remove the controller module

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

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

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

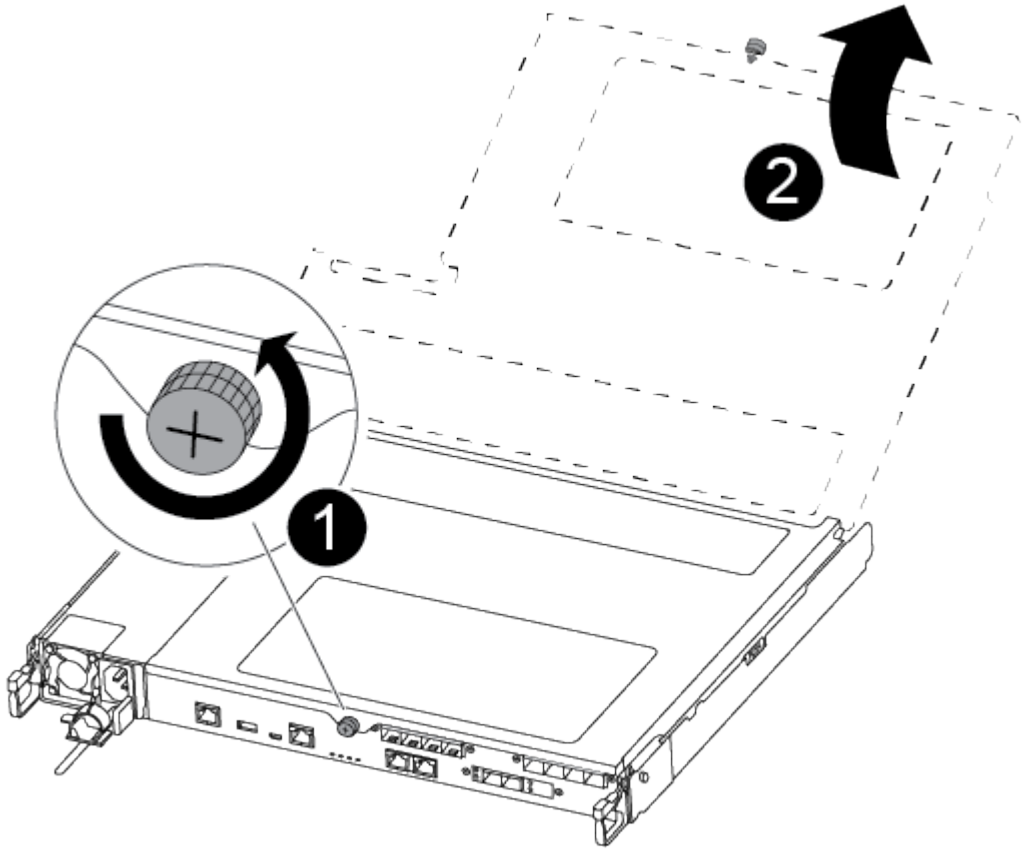
If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



1	Lever

2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover.

== Step 3: Replace the NVMEM battery

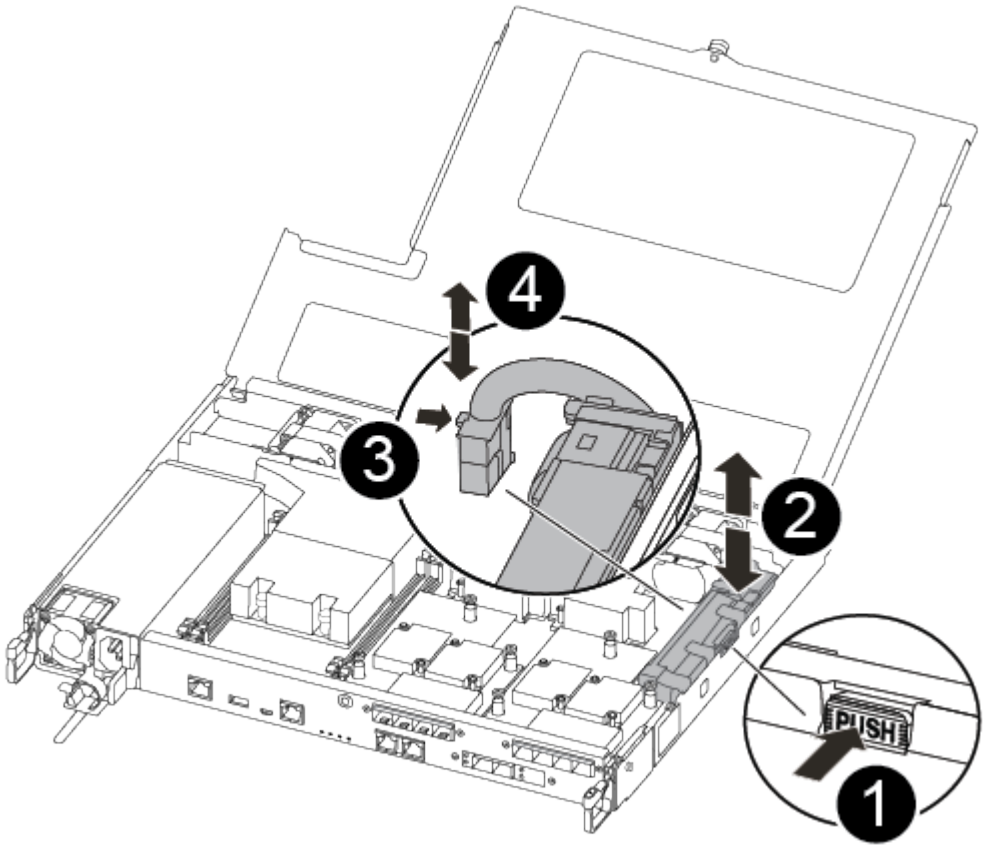
To replace the NVMEM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module.

Use the following video or the tabulated steps to replace the NVMEM battery:

Animation - Replace the NVMEM battery

1. Locate and replace the impaired NVMEM battery on your controller module.

It is recommended that you follow the illustrated instructions in the order listed.



1	Squeeze the clip on the face of the battery plug.
2	Unplug the battery cable from the socket.
3	Grasp the battery and press the blue locking tab marked PUSH.
4	Lift the battery out of the holder and controller module.

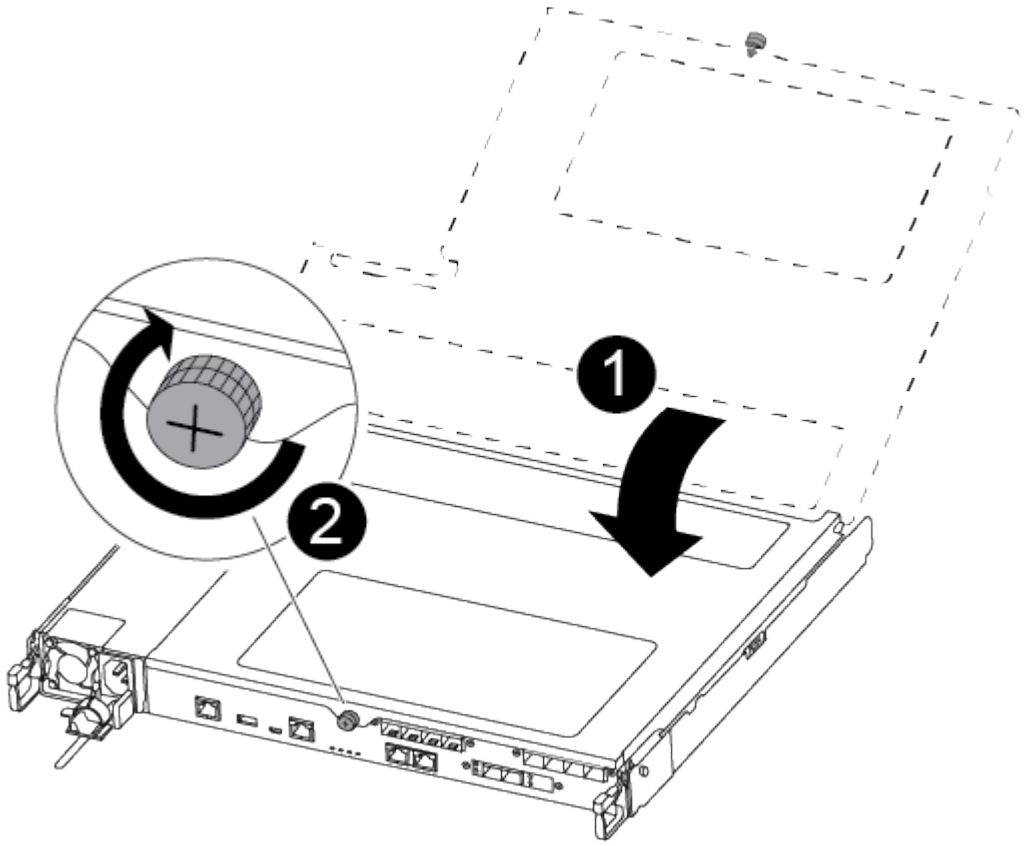
2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module and set it aside.
4. Remove the replacement NV battery from the antistatic shipping bag and align it to the battery holder.
5. Insert the replacement NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

== Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. Close the controller module cover and tighten the thumbscrew.



1	Controller module cover
2	Thumbscrew

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

The controller module should be fully inserted and flush with the edges of the chassis.

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

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

== Step 5: Return the failed part to NetApp

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

= Replace a power supply - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

Replacing a power supply (PSU) involves disconnecting the target PSU from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting it to the power source.

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

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

- Power supplies are auto-ranging.

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

Use the appropriate procedure for your type of PSU; AC or DC.

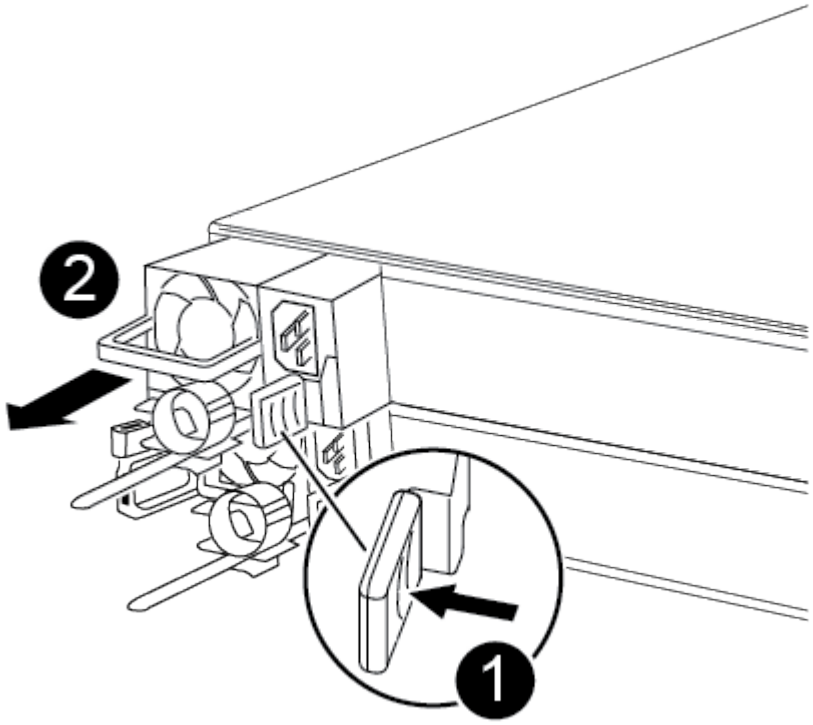
Option 1: Replace an AC PSU

Use the following video or the tabulated steps to replace the PSU:

Animation - Replace the AC PSU

1. If you are not already grounded, properly ground yourself.
2. Identify the PSU you want to replace, based on console error messages or through the red Fault LED on the PSU.
3. Disconnect the PSU:
   a. Open the power cable retainer, and then unplug the power cable from the PSU.
4. Remove the PSU by rotating the handle up, press the locking tab, and then pull the PSU out of the controller module.

> The PSU is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.



1	Blue PSU locking tab
2	Power supply

5. Install the replacement PSU in the controller module:
   a. Using both hands, support and align the edges of the PSU with the opening in the controller module.

b. Gently push the PSU into the controller module until the locking tab clicks into place.

The power supplies will only properly engage with the internal connector and lock in place one way.

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

6. Reconnect the PSU cabling:

   a. Reconnect the power cable to the PSU.

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

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

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

Option 2: Replace a DC PSU

To replace a DC PSU, complete the following steps.

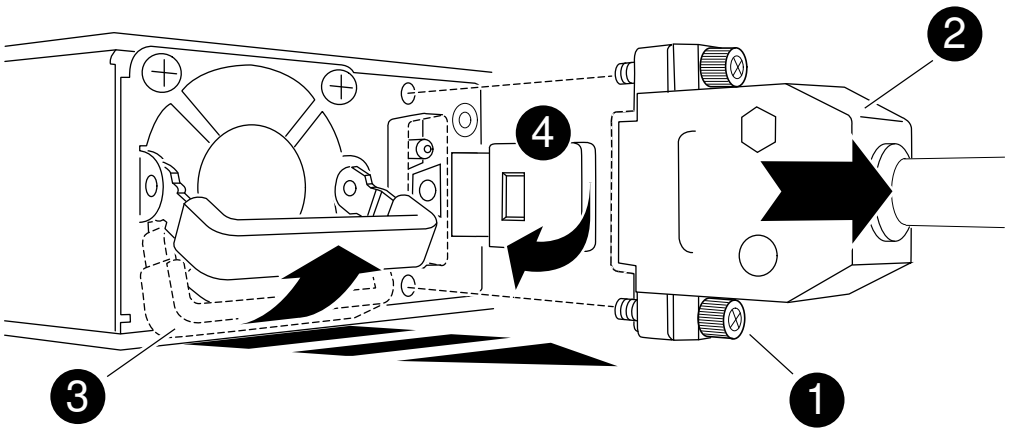
1. If you are not already grounded, properly ground yourself.
2. Identify the PSU you want to replace, based on console error messages or through the red Fault LED on the PSU.
3. Disconnect the PSU:

   a. Unscrew the D-SUB DC power cable connector using the thumb screws on the plug.

   b. Unplug the power cable from the PSU and set it aside.

4. Remove the PSU by rotating the handle up, press the locking tab, and then pull PSU out of the controller module.

The PSU is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.



❶	Thumb screws
❷	D-SUB DC power cable connector
❸	Power supply handle
❹	Blue PSU locking tab

5. Install the replacement PSU in the controller module:
   a. Using both hands, support and align the edges of the PSU with the opening in the controller module.
   b. Gently push the PSU into the controller module until the locking tab clicks into place.

      The power supplies will only properly engage with the internal connector and lock in place one way.

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

6. Reconnect the D-SUB DC power cable:
   a. Plug the power cable connector into the PSU.
   b. Secure the power cable to the PSU with the thumbscrews.

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

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

= Replace the real-time clock battery - ASA C250 :icons: font :relative_path: ./asa-c250/ :imagesdir: /tmp/d20240519-2754779-1ixwbok/source/./asa-c250/../media/

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 impaired controller SCSI blade. The `cluster kernel-service show` command

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=number_of_hours_downh`

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

== Step 2: Remove the controller module

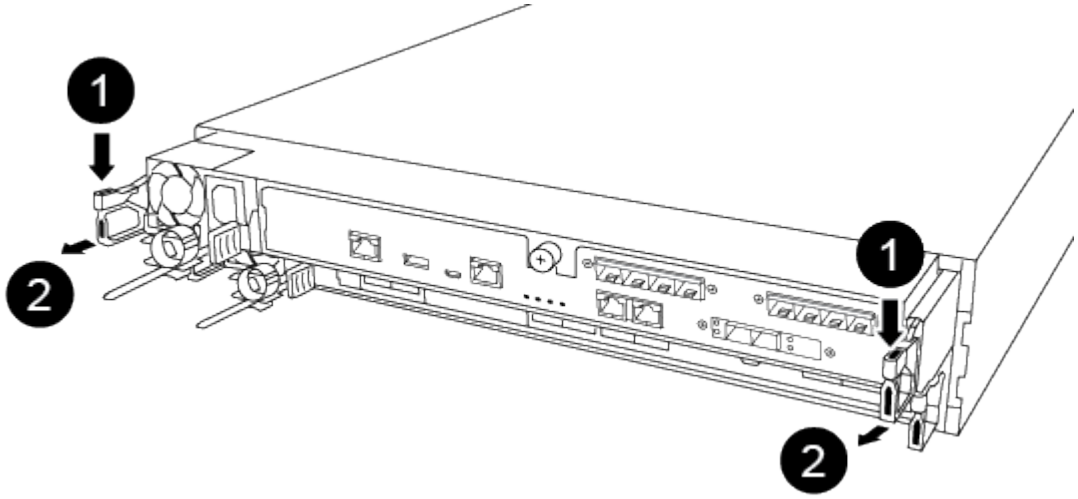
You must remove the controller module from the chassis when you replace a component inside the controller module.

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

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the

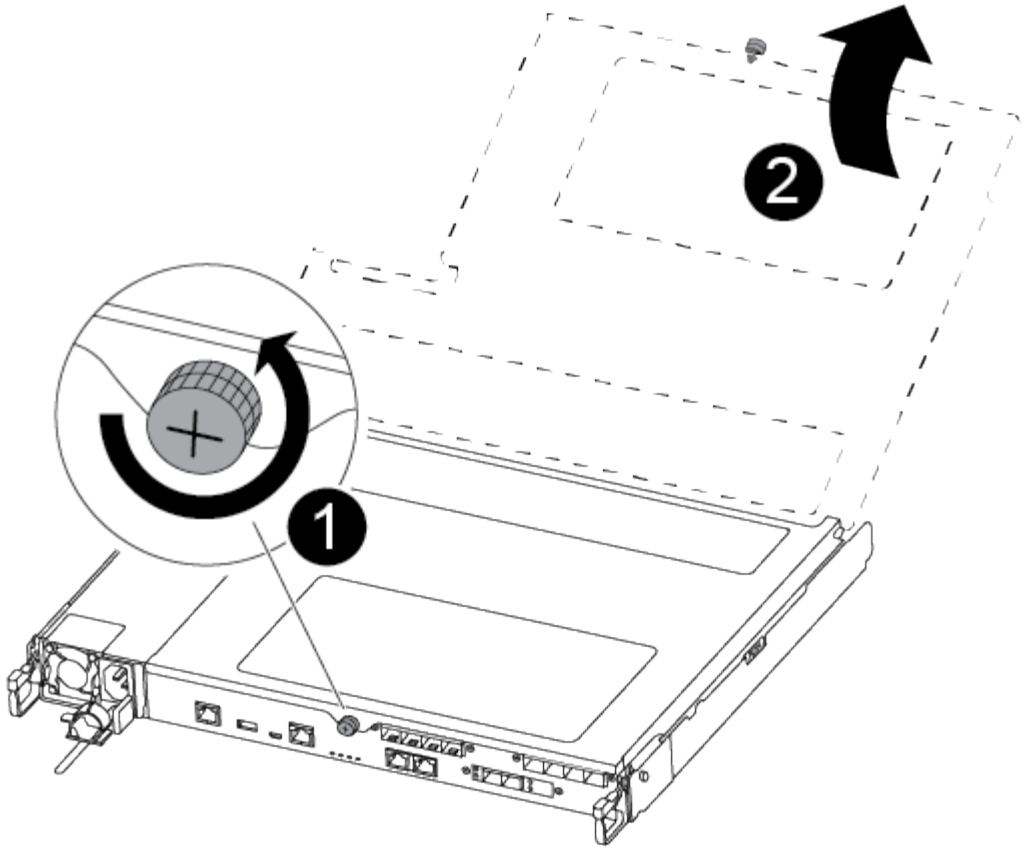
lever with your thumb, and gently pull the controller a few inches out of the chassis.

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



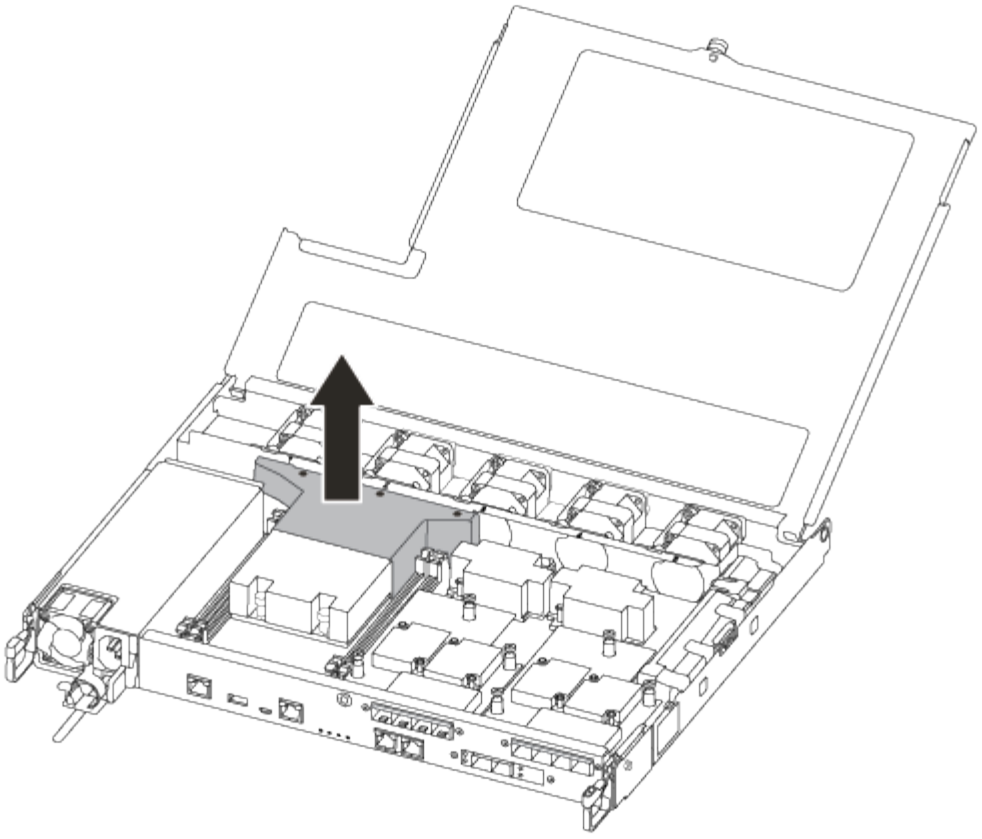
1	Lever
2	Latching mechanism

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.



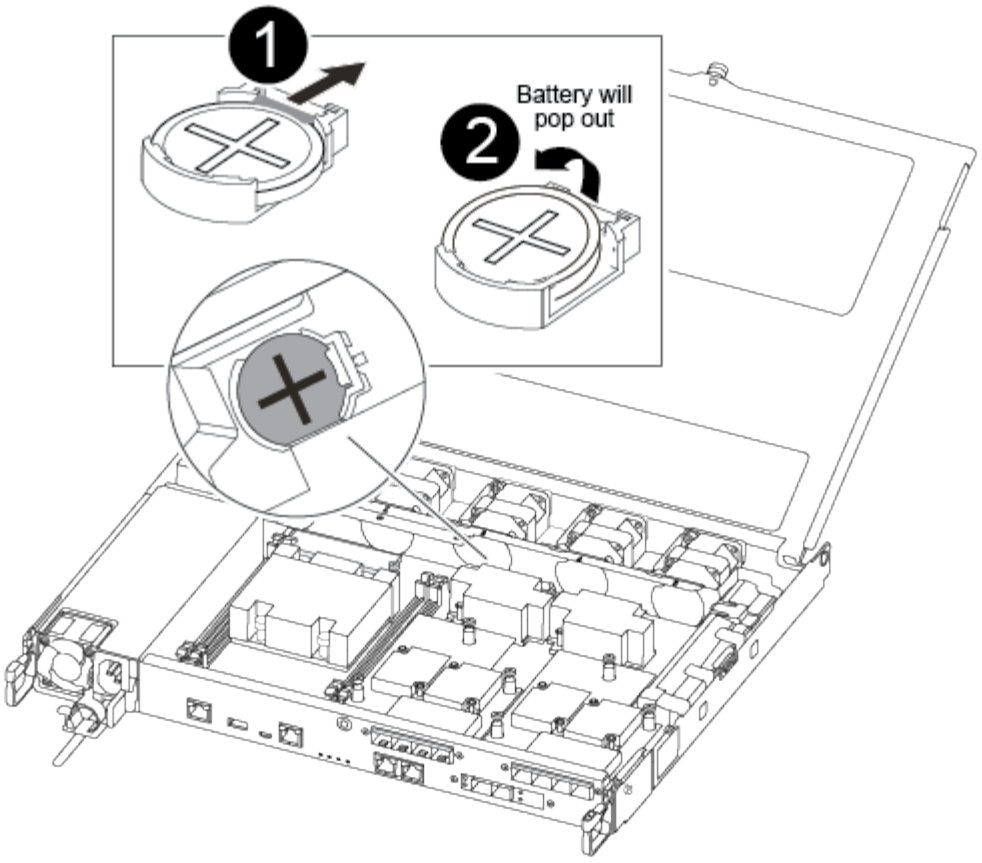
== Step 3: Replace the RTC battery

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

Use the following video or the tabulated steps to replace the RTC battery:

Animation - Replace the RTC battery

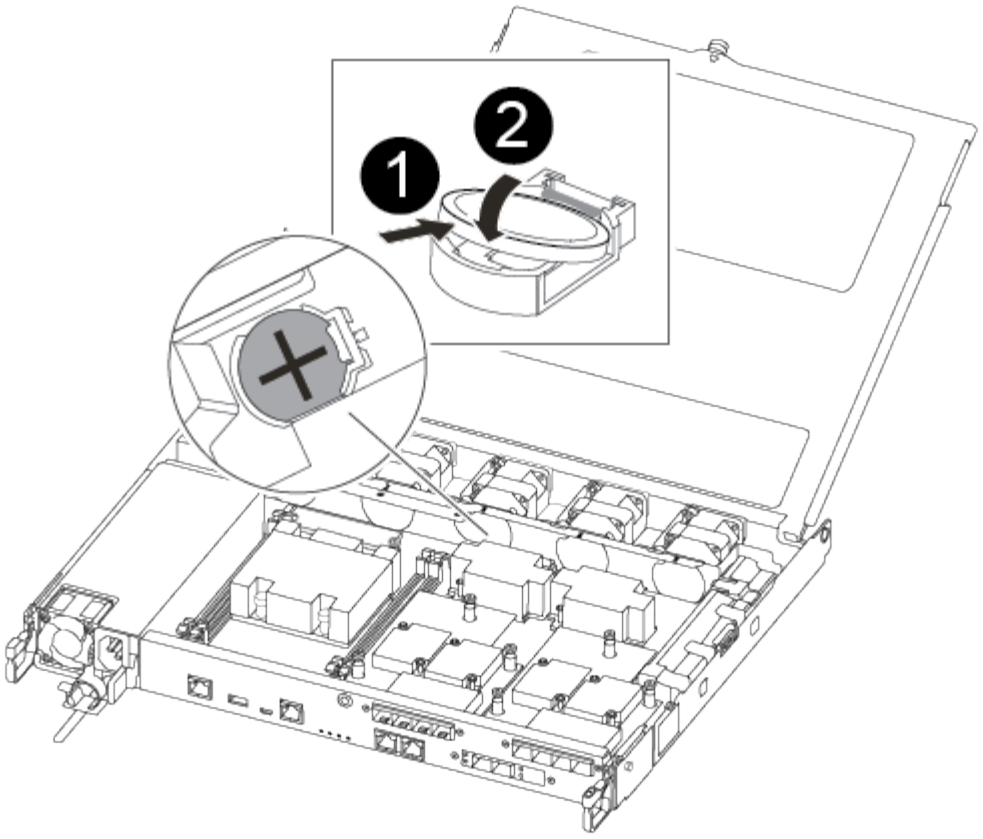
1. Locate the RTC battery between the heatsink and the midplane and remove it exactly as shown in the graphic.



1	Gently pull tab away from the battery housing. **Attention:** Pulling it away aggressively might displace the tab.
2	Lift the battery up. **Note:** Make a note of the polarity of the battery.
3	The battery should eject out.

The battery will be ejected out.

2. Remove the replacement battery from the antistatic shipping bag.
3. Locate the RTC battery holder between the heatsink and the midplane and insert it exactly as shown in the graphic.



1	With positive polarity face up, slide the battery under the tab of the battery housing.
2	Push the battery gently into place and make sure the tab secures it to the housing. Pushing it in aggressively might cause the battery to eject out again.

4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

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

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

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

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

3. Recable the system, as needed.

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

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   f. Halt the controller at the LOADER prompt.

   The controller module should be fully inserted and flush with the edges of the chassis.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

== Step 5: Return the failed part to NetApp

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

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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