Maintain

ONTAP Systems

NetApp
April 25, 2022

Table of Contents

Maintain

Boot media

Overview of boot media replacement - AFF A700s

The primary boot media stores the ONTAP boot image that the system uses when it boots. You can restore the primary boot media image by using the ONTAP image on the secondary boot media, or if necessary, by using a USB flash drive.

If your secondary boot media has failed or is missing the image.tgz file, you must restore the primary boot media using a USB flash drive. The drive must be formatted to FAT32 and must have the appropriate amount of storage to hold the image_xxx.tgz file.

- The replacement process restores the var file system from the secondary boot media or USB flash drive to the primary boot media.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

Check onboard encryption keys - AFF A700s

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

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

Steps

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

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner

controller if the impaired controller is down, using the `version -v` command:

- If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to [Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier].
- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later].

4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

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

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

Steps

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

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

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

Verify NVE configuration

Steps

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

      If the command fails, contact NetApp Support.

mysupport.netapp.com

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

c. Shut down the impaired controller.

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

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

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

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

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

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

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

Verify NSE configuration

Steps

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

- If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
- If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
- If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.
   b. If the `Restored` column displays anything other than `yes`:
      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

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

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

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

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

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

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

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

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

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

Verify NVE configuration

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

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

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

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

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

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

c. Shut down the impaired controller.

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

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

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

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

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

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

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

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

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

   h. You can safely shut down the controller.

Verify NSE configuration

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

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

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

yes, you need to complete some additional steps.

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

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

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

      mysupport.netapp.com

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

Shut down the controller - AFF A700s

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

Replace the boot media - AFF A700s

You must remove the controller module from the chassis, open it, and then replace the failed boot media.

Step 1: Remove the controller module

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

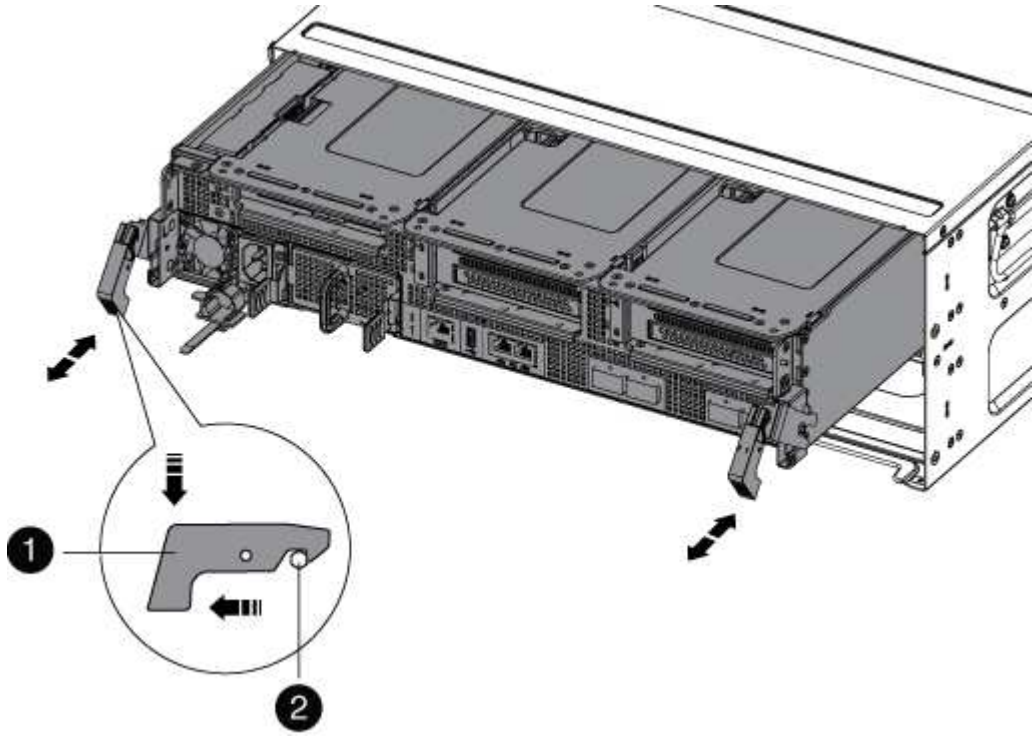
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.

5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

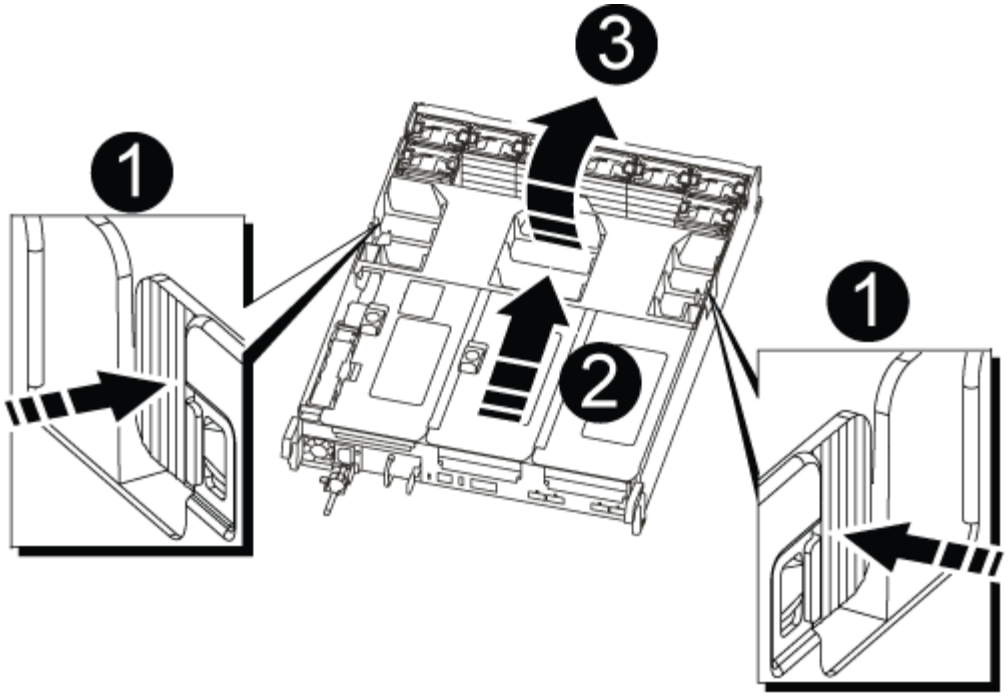


1	Locking latch
2	Locking pin

1. Slide the controller module out of the chassis.

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

2. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



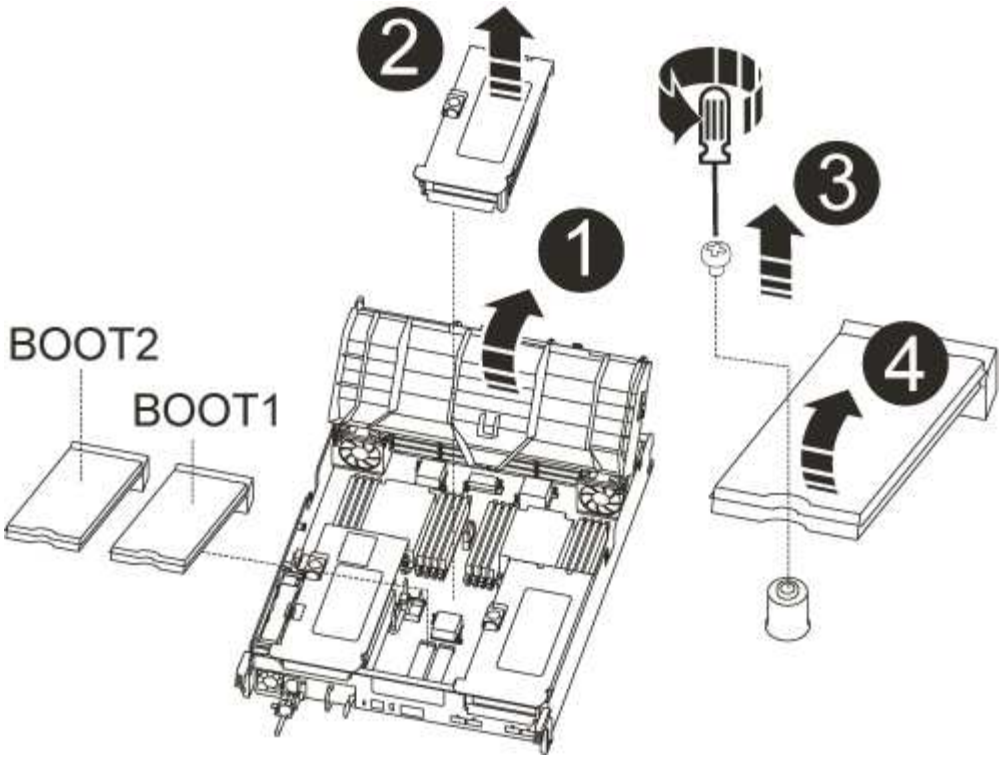
1	Air duct locking tabs
2	Risers
3	Air duct

Step 2: Replace the boot media - AFF A700s

You must locate the failed boot media in the controller module by removing the middle PCIe module on the controller module, locate the failed boot media by the lit LED near the boot media, and then replace the boot media.

You need a Phillips head screwdriver to remove the screw that holds the boot media in place.

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media:
   a. Open the air duct, if needed.
   b. If needed, remove Riser 2, the middle PCIe module, by unlocking the locking latch and then removing the riser from the controller module.



1	Air duct
2	Riser 2 (middle PCIe module)
3	Boot media screw
4	Boot media

3. Locate the failed boot media by the lit LED on the controller module motherboard.
4. Remove the boot media from the controller module:
   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
5. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
6. Check the boot media to make sure that it is seated squarely and completely in the socket.

   If necessary, remove the boot media and reseat it into the socket.
7. Rotate the boot media down until it is flush with the motherboard.
8. Secure the boot media in place by using the screw.

Do not over-tighten the screw. Doing so might crack the boot media circuit board.

9. Reinstall the riser into the controller module.
10. Close the air duct:
    a. Rotate the air duct downward.
    b. Slide the air duct toward the risers until it clicks into place.

Transfer the boot image to the boot media - AFF A700s

You can install the system image to the replacement boot media using by using either the image on second boot media installed in the controller module, the primary method to restore the system image, or by transferring the boot image to the boot media using a USB flash drive when the secondary boot media restore failed or if the image.tgz file is not found on the secondary boot media.

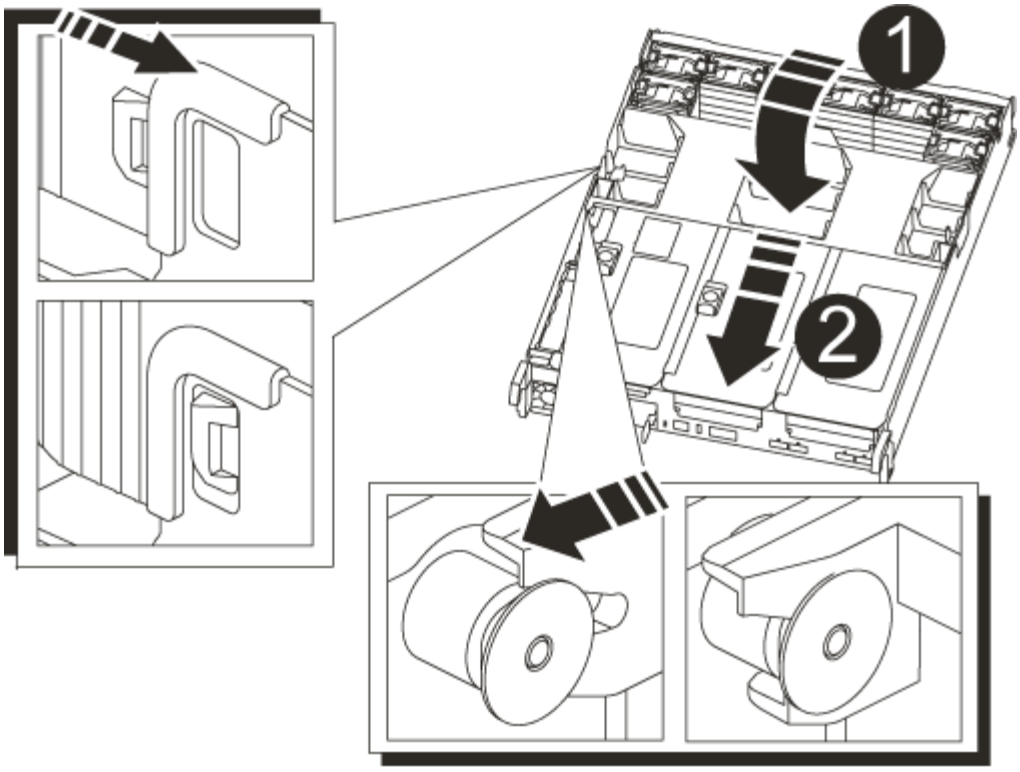
Option 1: Transfer files to the boot media using backup recovery from the second boot media

You can install the system image to the replacement boot media using the image on second boot media installed in the controller module. This is the primary method for transferring the boot media files to the replacement boot media in systems with two boot media in the controller module.

The image on the secondary boot media must contain an `image.tgz` file and must not be reporting failures. If image.tgz file is missing or the boot media reports failures, you cannot use this procedure. You must transfer the boot image to the replacement boot media using the USB flash drive replacement procedure.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
    a. Swing the air duct all the way down to the controller module.
    b. Slide the air duct toward the risers until the locking tabs click into place.
    c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Air duct
2	Risers

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

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

5. Recable the power supply, and then connect it to the power source.

   Make sure that you reattach the power cable locking collar on the power cord.

6. Gently push the controller module all the way into the system until the controller module locking hooks begin to rise, firmly push on the locking hooks to finish seating the controller module, and then swing the locking hooks into the locked position over the pins on the controller module.

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

7. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

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

8. From the LOADER prompt, boot the recovery image from the secondary boot media: `boot_recovery`

   The image is downloaded from the secondary boot media.

9. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
10. After the image is installed, start the restoration process:
    a. Record the IP address of the impaired controller that is displayed on the screen.
    b. Press `y` when prompted to restore the backup configuration.
    c. Press `y` when prompted to confirm that the backup procedure was successful.
11. From the partner controller in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address` *`impaired_node_IP_address`*
12. After the configuration synchronization is complete without errors, press `y` when prompted to confirm that the backup procedure was successful.
13. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.
14. Exit advanced privilege level on the healthy controller.

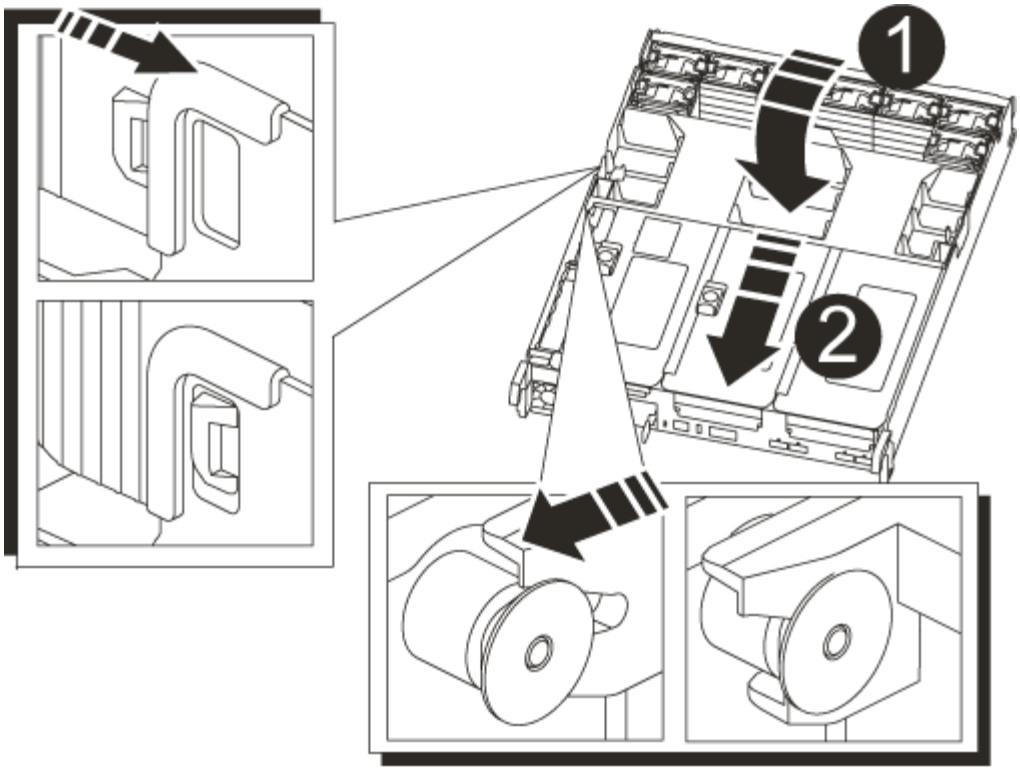
Option 2: Transfer the boot image to the boot media using a USB flash drive

This procedure should only be used if the secondary boot media restore failed or if the image.tgz file is not found on the secondary boot media.

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

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
    a. Swing the air duct all the way down to the controller module.
    b. Slide the air duct toward the risers until the locking tabs click into place.
    c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Air duct
2	Risers

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

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

5. Recable the power supply, and then connect it to the power source.

   Make sure that you reattach the power cable locking collar on the power cord.

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

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

7. Gently push the controller module all the way into the system until the controller module locking hooks begin to rise, firmly push on the locking hooks to finish seating the controller module, and then swing the locking hooks into the locked position over the pins on the controller module.

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

8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

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

9. Although the environment variables and bootargs are retained, you should check that all required boot environment variables and bootargs are properly set for your system type and configuration using the `printenv bootarg name` command and correct any errors using the `setenv variable-name <value>` command.
   a. Check the boot environment variables:
      - `bootarg.init.boot_clustered`
      - `partner-sysid`
      - `bootarg.init.flash_optimized` for AFF C190/AFF A220 (All Flash FAS)
      - `bootarg.init.san_optimized` for AFF A220 and All SAN Array
      - `bootarg.init.switchless_cluster.enable`
   b. If External Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:
      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `kmip.init.interface <value>`
      - `kmip.init.ipaddr <value>`
      - `kmip.init.netmask <value>`
      - `kmip.init.gateway <value>`
   c. If Onboard Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:
      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `bootarg.onboard_keymanager <value>`
   d. Save the environment variables you changed with the `savenv` command
   e. Confirm your changes using the `printenv *variable-name*` command.
10. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

    The image is downloaded from the USB flash drive.
11. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
12. After the image is installed, start the restoration process:
    a. Record the IP address of the impaired controller that is displayed on the screen.
    b. Press `y` when prompted to restore the backup configuration.
    c. Press `y` when prompted to confirm that the backup procedure was successful.
13. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.
14. From the partner controller in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address *impaired_node_IP_address*`

15. After the configuration synchronization is complete without errors, press `y` when prompted to confirm that the backup procedure was successful.
16. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.
17. Verify that the environmental variables are set as expected.
    a. Take the controller to the LOADER prompt.

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

    b. Check the environment variable settings with the `printenv` command.
    c. If an environment variable is not set as expected, modify it with the `setenv` *`environment-variable-name changed-value`* command.
    d. Save your changes using the `savenv` command.
    e. Reboot the controller.
18. With the rebooted impaired controller displaying the `Waiting for giveback…` message, perform a giveback from the healthy controller:

If your system is in…	Then…
An HA pair	After the impaired controller is displaying the `Waiting for giveback…` message, perform a giveback from the healthy controller: a. From the healthy controller: `storage failover giveback -ofnode partner_node_name` The impaired controller takes back its storage, finishes booting, and then reboots and is again taken over by the healthy controller. If the giveback is vetoed, you can consider overriding the vetoes. ONTAP 9 High-Availability Configuration Guide b. Monitor the progress of the giveback operation by using the `storage failover show-giveback` command. c. After the giveback operation is complete, confirm that the HA pair is healthy and that takeover is possible by using the `storage failover show` command. d. Restore automatic giveback if you disabled it using the `storage failover modify` command.

19. Exit advanced privilege level on the healthy controller.

Boot the recovery image - AFF A700s

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

the environmental variables.

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

   The image is downloaded from the USB flash drive.

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

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

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

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

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

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

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

Restore OKM, NSE, and NVE as needed - AFF A700s

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

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

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

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

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

Steps

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

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

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

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

   Example of backup data:

   ```
   -----------------------BEGIN BACKUP-----------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
   IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . . .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

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

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

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

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

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

  Terminating CIFS can cause loss of data.

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

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

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

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

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

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

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

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

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

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

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

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

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

Steps

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

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

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

     Terminating CIFS can cause loss of data.

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

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

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

8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

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

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

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

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

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

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

Steps

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

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

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

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

     Terminating CIFS can cause loss of data.

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

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

      If the command fails, contact Customer Support.

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

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

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

Return the failed part to NetApp - AFF A700s

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 - AFF A700s

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

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

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

Shut down the controllers - AFF A700s

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

About this task

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

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

Steps

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

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

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

   The confirmation message looks like the following:

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

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

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

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

   Answer `y` when prompted.

Replace hardware - AFF A700s

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

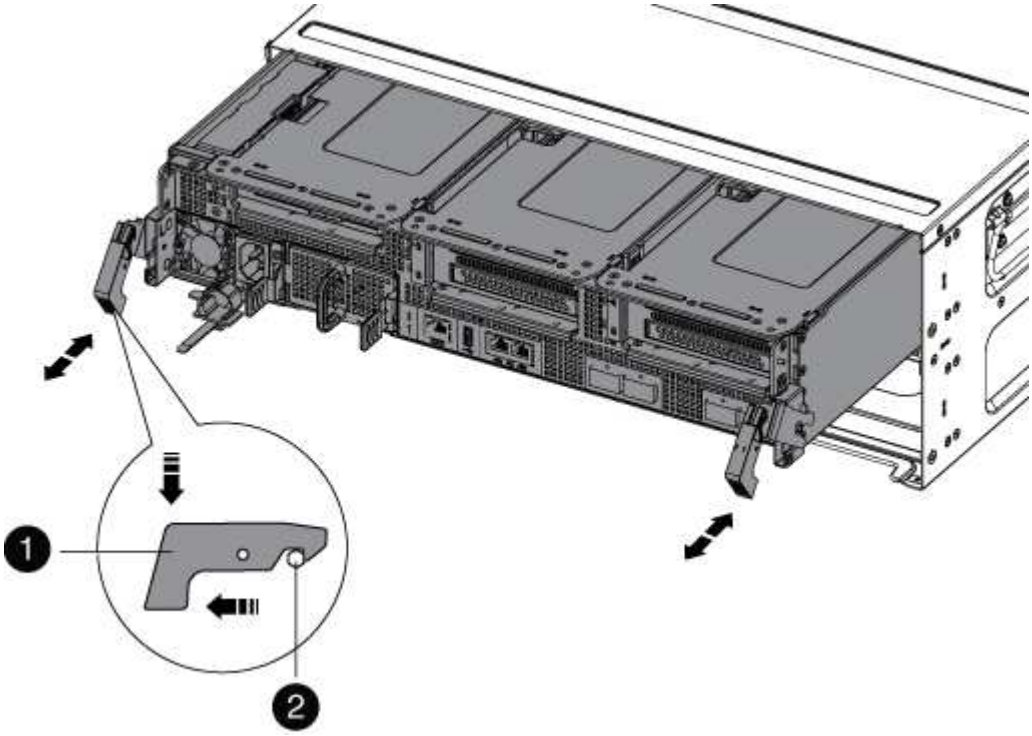
Step 1: Remove the controller modules

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

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

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.



1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.
7. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

Step 2: Move drives to the new chassis

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

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

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

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

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

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

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

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

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

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

Step 4: Install the controllers

After you install the controller module into the new chassis, boot it to a state where you can run the diagnostic

test.

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

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

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

3. Recable the console to the controller module, and then reconnect the management port.
4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

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

Complete the restoration and replacement process - AFF A700s

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

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

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

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

   The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:

a. Set the HA state for the chassis: `ha-config modify chassis HA-state`

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

   - `ha`
   - `non-ha`

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

3. If you have not already done so, recable the rest of your system.
4. Reinstall the bezel on the front of the system.

Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `system node halt -node node_name`

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

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Step 3: Return the failed part to NetApp

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 - AFF A700s

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

- All drive shelves must be working properly.
- The healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).

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

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

Shut down the impaired controller - AFF A700s

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

About this task

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

Steps

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

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

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

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

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

Replace the ontroller module hardware - AFF A700s

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

Step 1: Remove the controller module

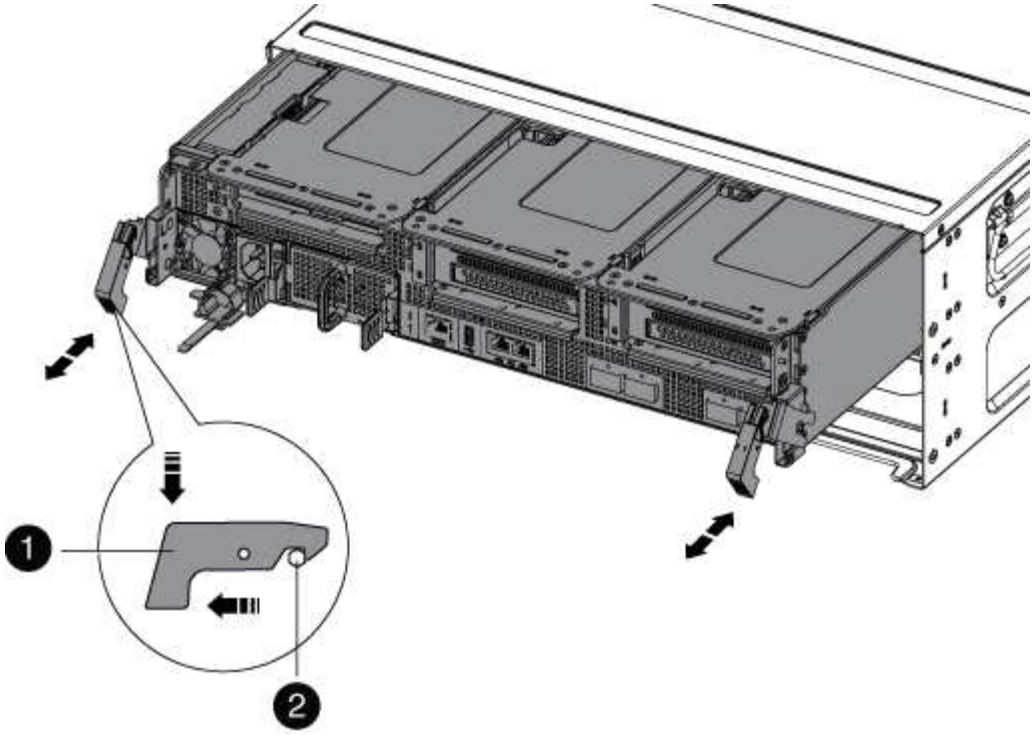
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

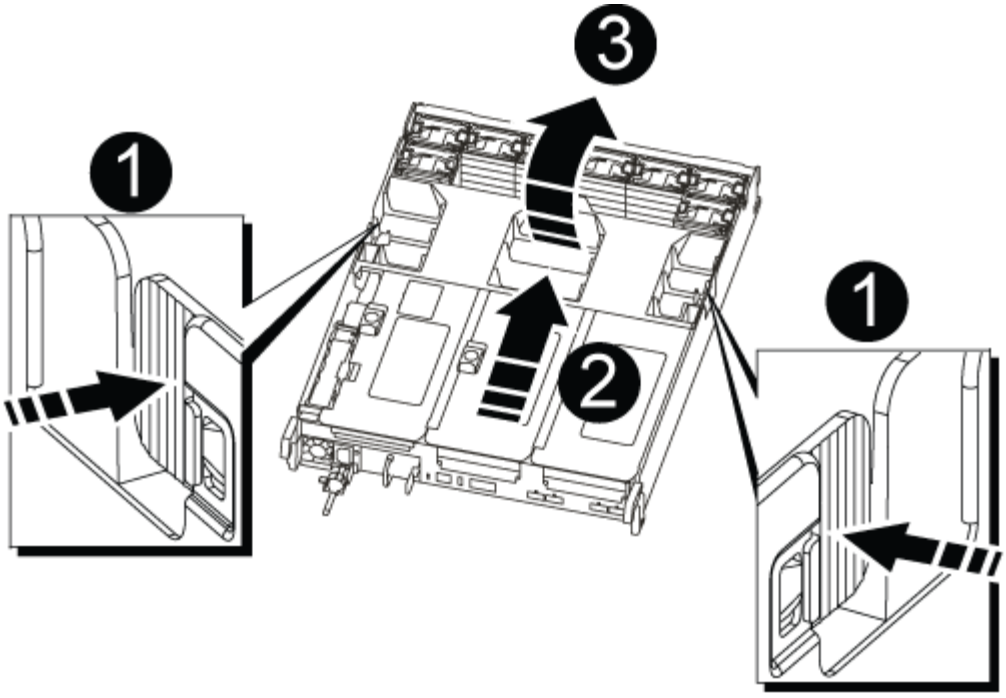


1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

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

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



1	Air duct locking tabs
2	Risers
3	Air duct

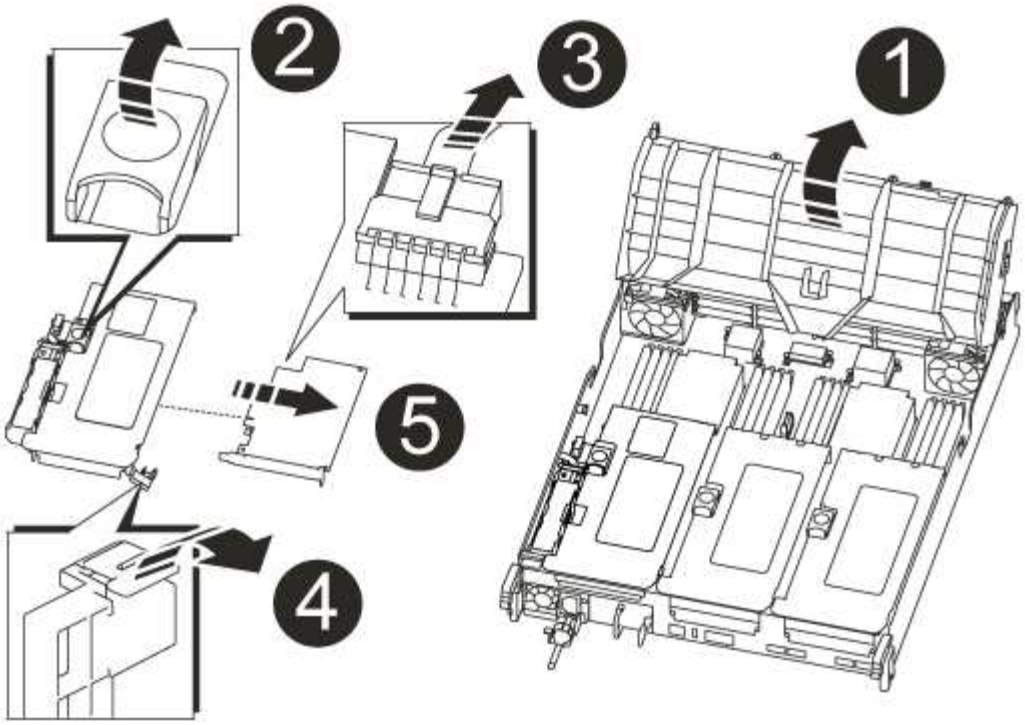
Step 2: Move the NVRAM card

As part of the controller replacement process, you must remove the NVRAM card from Riser 1 in the impaired controller module and install the card into Riser 1 of the replacement controller module. You should only reinstall Riser 1 into the replacement controller module after you have moved the DIMMs from the impaired controller module to the replacement controller module.

1. Remove the NVRAM riser, Riser 1, from the controller module:
   a. Rotate the riser locking latch on the left side of the riser up and toward the fans.

      The NVRAM riser raises up slightly from the controller module.

   b. Lift the NVRAM riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser straight up out of the controller module, and then place it on a stable, flat surface so that you can access the NVRAM card.



1	Air duct
2	Riser 1 locking latch
3	NVRAM battery cable plug connecting to the NVRAM card
4	Card locking bracket
5	NVRAM card

2. Remove the NVRAM card from the riser module:
   a. Turn the riser module so that you can access the NVRAM card.
   b. Unplug the NVRAM battery cable that is attached to the NVRAM card.
   c. Press the locking bracket on the side of the NVRAM riser, and then rotate it to the open position.
   d. Remove the NVRAM card from the riser module.
3. Remove the NVRAM riser from the replacement controller module.
4. Install the NVRAM card into the NVRAM riser:
   a. Align the card with the card guide on the riser module and the card socket in the riser.
   b. Slide the card squarely into the card socket.

   Make sure that the card is completely and squarely seated into the riser socket.

c. Connect the battery cable to the socket on the NVRAM card.

d. Swing the locking latch into the locked position and make sure that it locks in place.

Step 3: Move PCIe cards

As part of the controller replacement process, you must remove both PCIe riser modules, Riser 2 (the middle riser) and Riser 3 (riser on the far right) from the impaired controller module, remove the PCIe cards from the riser modules, and install them in the same riser modules in the replacement controller module. You will install the riser modules into the replacement controller module once the DIMMs have been moved to the replacement controller module.

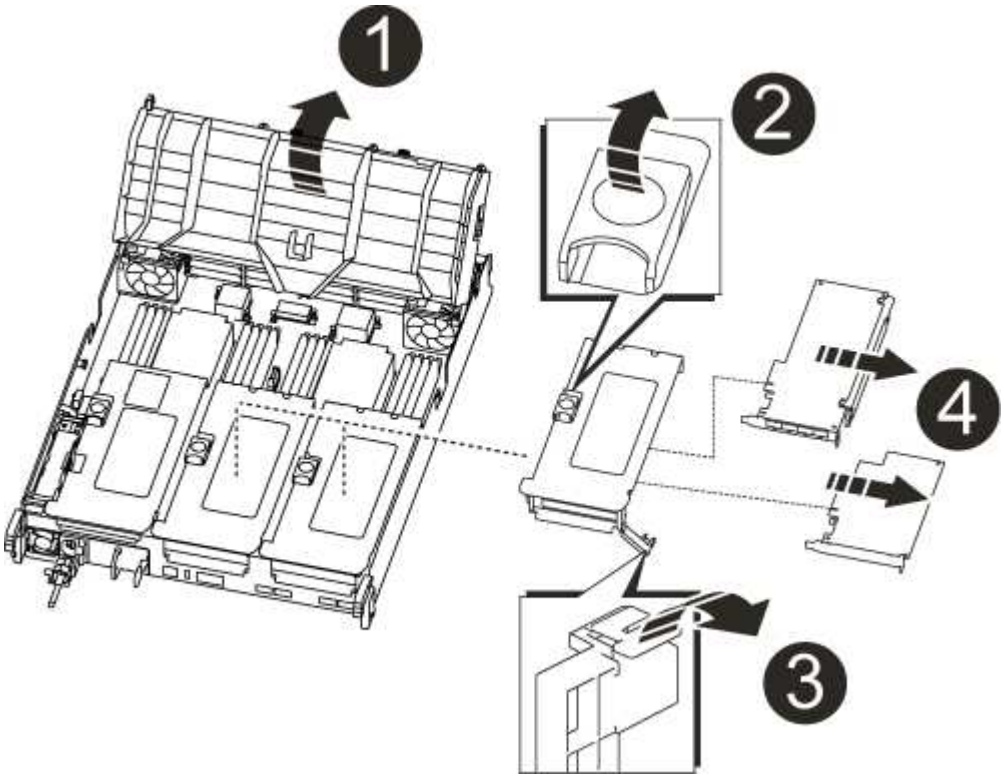
1. Remove the PCIe riser from the controller module:

   a. Remove any SFP modules that might be in the PCIe cards.

   b. Rotate the module locking latch on the left side of the riser up and toward the fan modules.

      The PCIe riser raises up slightly from the controller module.

   c. Lift the PCIe riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.



1	Air duct
2	Riser locking latch
3	Card locking bracket

4	Riser 2 (middle riser) and PCI cards in riser slots 2 and 3.

2. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. Remove the PCIe card from the riser.
3. Remove the corresponding riser from the replacement controller module.
4. Install the PCIe card into the same slot in PCIe riser:
   a. Align the card with the card guide on the riser and the card socket in the riser, and then slide it squarely into the socket in the riser.

      Make sure that the card is completely and squarely seated into the riser socket.

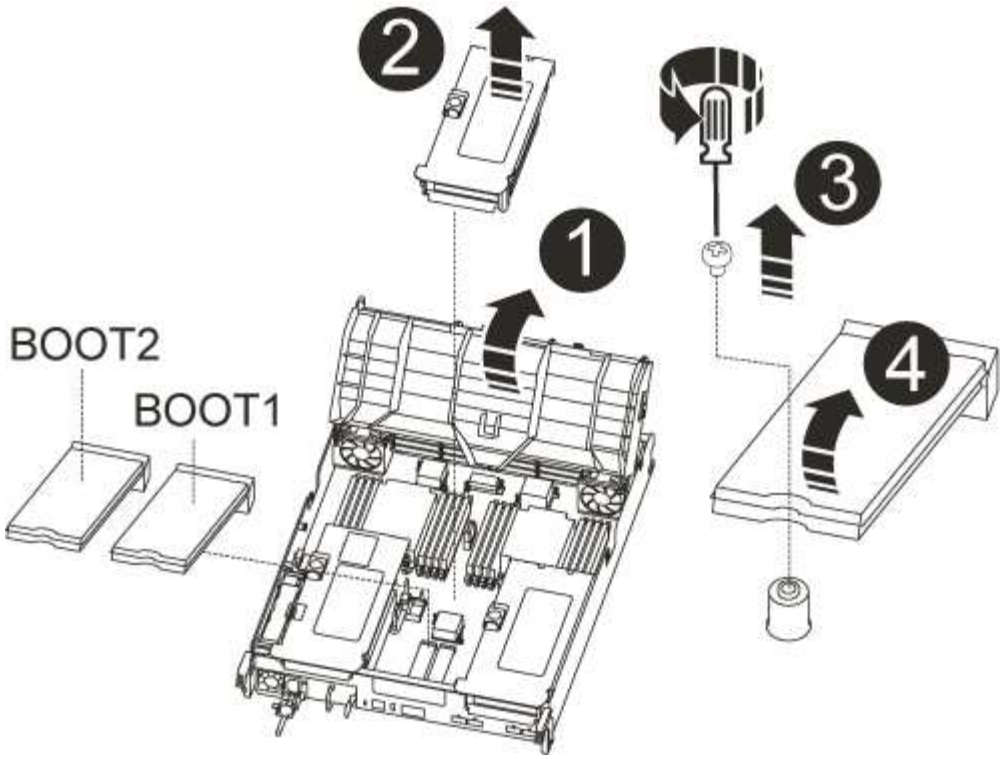
   b. Swing the locking latch into place until it clicks into the locked position.
5. Repeat the preceding steps for Riser 3 and PCIe cards in slots 4 and 5 in the impaired controller module.

Step 4: Move the boot media

There are two boot media devices in the AFF A700s, a primary and a secondary or backup boot media. You must move them from the impaired controller to the *replacement* controller and install them into their respective slots in the *replacement* controller.

The boot media are located under Riser 2, the middle PCIe riser module. This PCIe module must be removed to gain access to the boot media.

1. Locate the boot media:
   a. Open the air duct, if needed.
   b. If needed, remove Riser 2, the middle PCIe module, by unlocking the locking latch and then removing the riser from the controller module.



+

1	Air duct
2	Riser 2 (middle PCIe module)
3	Boot media screw
4	Boot media

2. Remove the boot media from the controller module:
   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
3. Move the boot media to the new controller module and install it:

> Install the boot media into the same socket in the replacement controller module as it was installed in the impaired controller module; primary boot media socket (slot 1) to primary boot media socket, and secondary boot media socket (slot 2) to secondary boot media socket.

   a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.

b. Rotate the boot media down toward the motherboard.

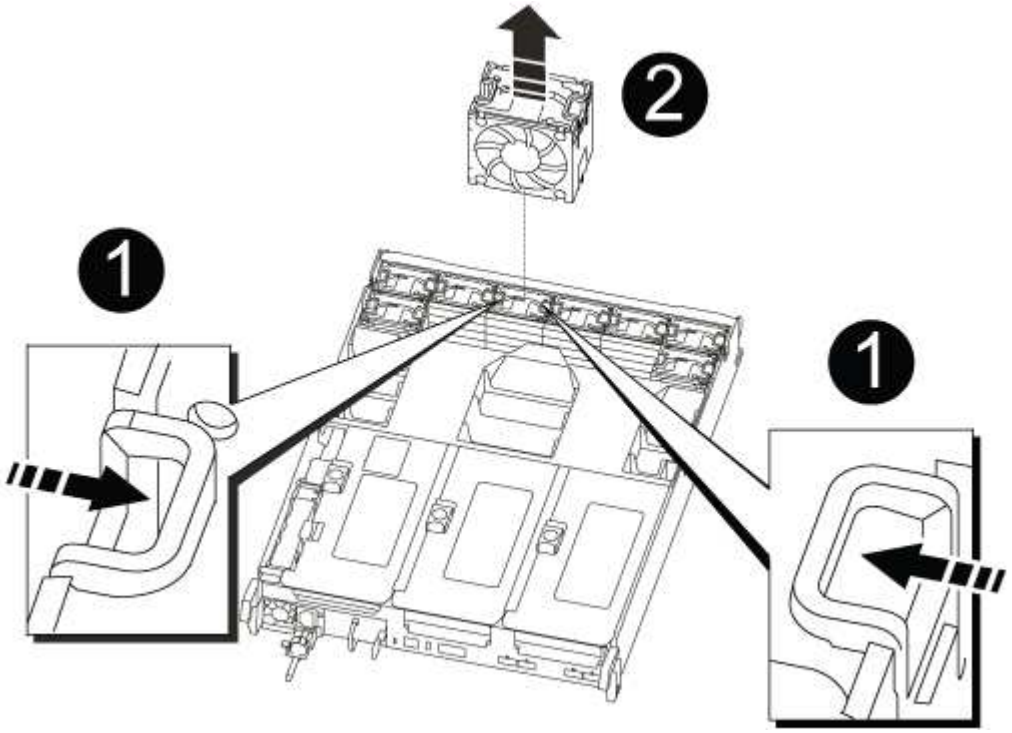
c. Secure the boot media to the motherboard using the boot media screw.

   Do not over-tighten the screw or you might damage the boot media.

Step 5: Move the fans

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

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



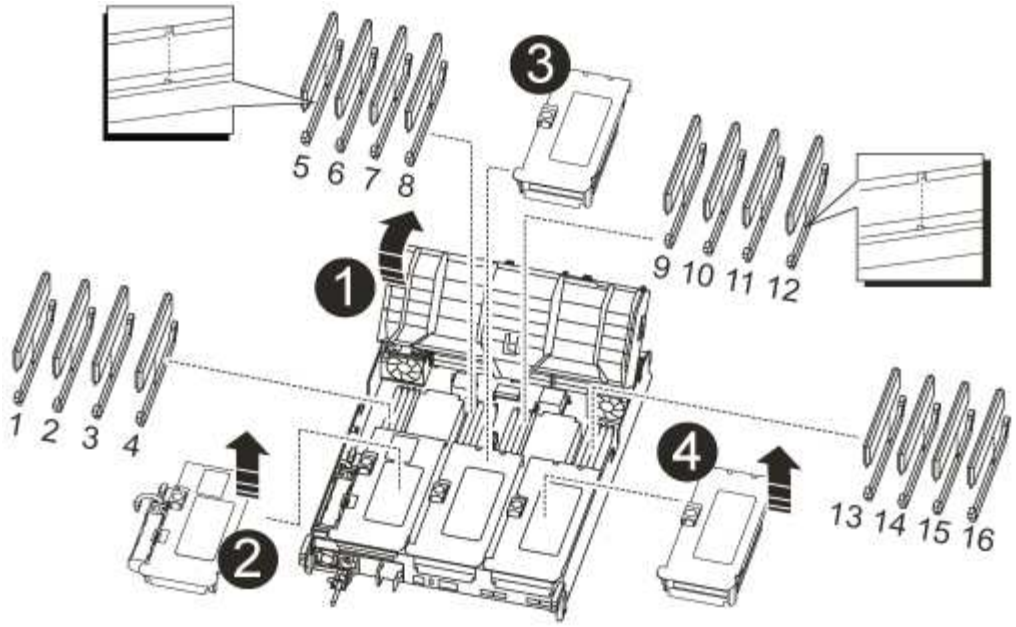
1	Fan locking tabs
2	Fan module

2. Move the fan module to the replacement controller module, and then install the fan module by aligning its edges with the opening in the controller module, and then sliding the fan module into the controller module until the locking latches click into place.
3. Repeat these steps for the remaining fan modules.

Step 6: Move system DIMMs

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

1. Locate the DIMMs on your controller module.



1	Air duct
2	Riser 1 and DIMM bank 1-4
3	Riser 2 and DIMM banks 5-8 and 9-12
4	Riser 3 and DIMM bank 13-16

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

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

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

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

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

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

Step 7: Install the NVRAM module

To install the NVRAM module, you must follow the specific sequence of steps.

1. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

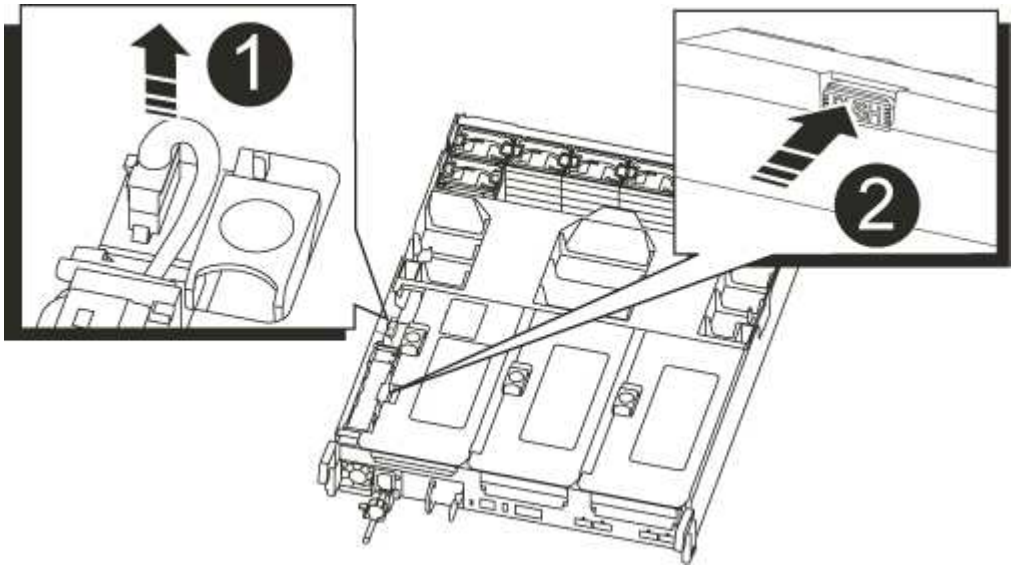
      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP modules that were removed from the PCIe cards.

Step 8: Move the NVRAM battery

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

1. Locate the NVRAM battery on the left side of the riser module, Riser 1.



1	NVRAM battery plug
2	Blue NVRAM battery locking tab

2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Move the battery pack to the replacement controller module, and then install it in the NVRAM riser:
   a. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook

into the slots on the battery pack, and the battery pack latch engages and locks into place.

b. Press firmly down on the battery pack to make sure that it is locked into place.

c. Plug the battery plug into the riser socket and make sure that the plug locks into place.

Step 9: Install a PCIe riser

To install a PCIe riser, you must follow a specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

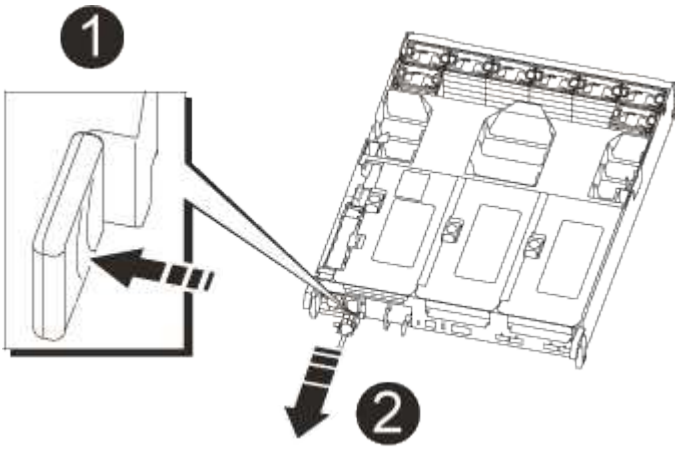
   d. Reinsert any SFP modules that were removed from the PCIe cards.
3. Repeat the preceding steps for Riser 3 and PCIe cards in slots 4 and 5 in the impaired controller module.

Step 10: Move the power supply

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

1. If you are not already grounded, properly ground yourself.
2. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

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



1	Blue power supply locking tab

2	Power supply

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

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

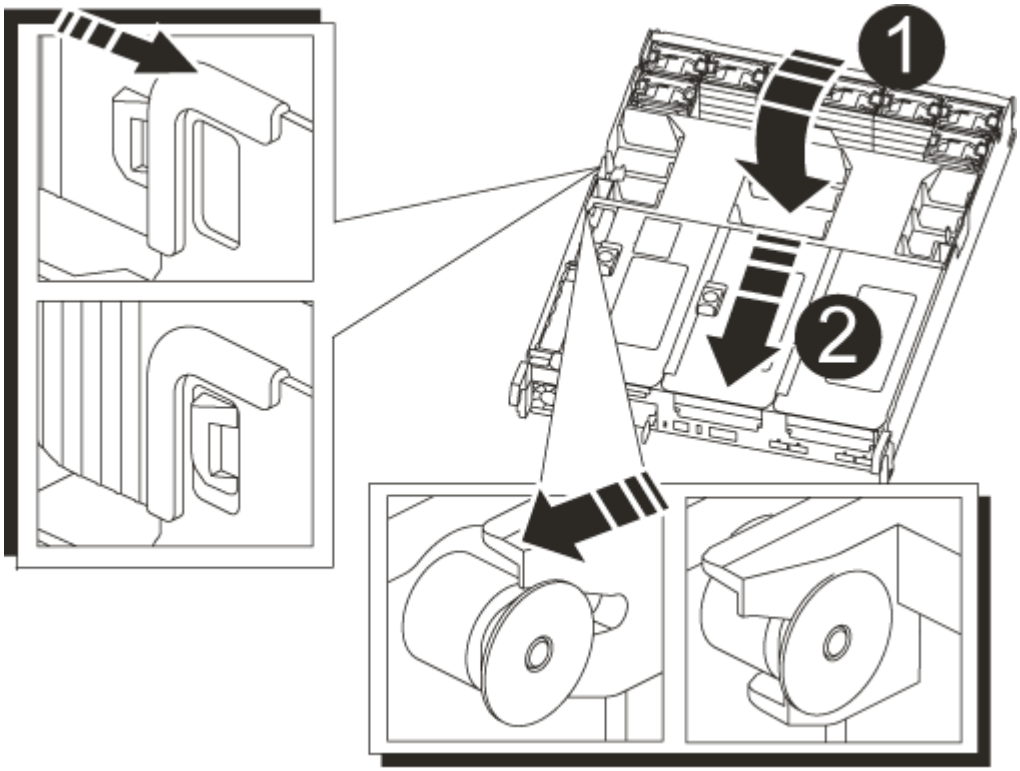
   To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

5. Remove the PSU blanking panel from the impaired controller module, and then install it in the replacement controller module.

Step 11: Install the controller module

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

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.



+

1	Locking tabs
2	Slide plunger

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

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

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

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

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
   e. Select the option to boot to Maintenance mode from the displayed menu.
7. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the nicadmin convert command from Maintenance mode.

   Be sure to exit Maintenance mode after completing the conversion.

Restore and verify the system configuration - AFF A700s

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

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

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

About this task

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

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

Steps

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

   The date and time are given in GMT.

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

   The date and time are given in GMT.

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

   The date and time are given in GMT.

Step 2: Verify and set the HA state of the chassis

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

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

   The HA state should be the same for all components.

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

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

   - ha
   - non-ha

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

Step 3: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

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

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

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

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

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

Recable the system and reassign disks - AFF A700s

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

Step 1: Recable the system

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

Steps

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

Step 2: Reassign disks

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

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

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

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

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

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

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

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

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

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

`giveback -ofnode replacement_node_name`

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

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

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

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

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

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

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

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

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

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

Complete system restoration - AFF A700s

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

Step 1: Install licenses for the replacement node in ONTAP

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

About this task

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

Before you begin

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

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

Steps

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

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

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

Step 2: Restore Storage and Volume Encryption functionality

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

Step

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

Step 3: Verify LIFs and registering the serial number

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

Steps

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

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

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

Step 4: Return the failed part to NetApp

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

Replace a DIMM - AFF A700s

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

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

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

Shut down the impaired controller

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

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

ONTAP 9 System Administration Reference

Steps

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

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

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

Remove the controller module

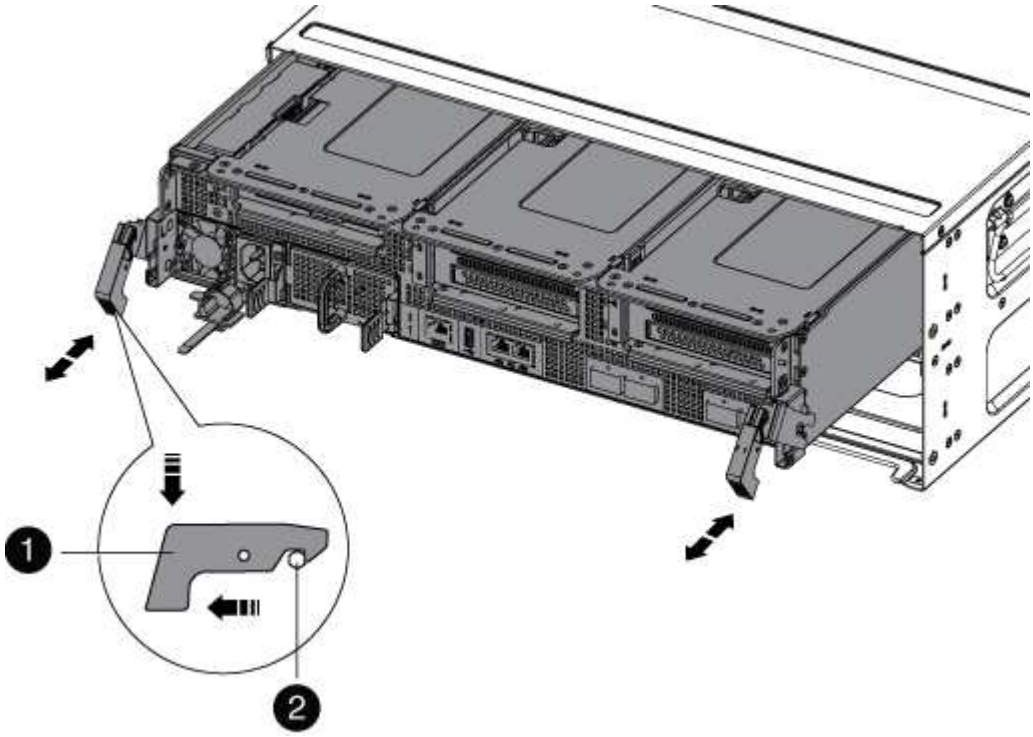
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

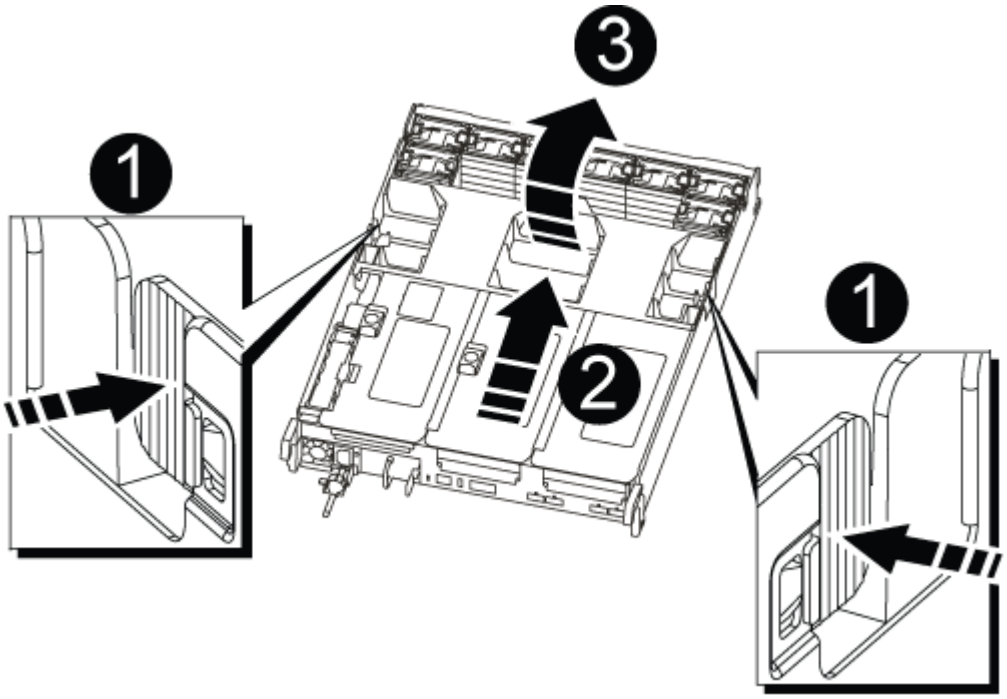


1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

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

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

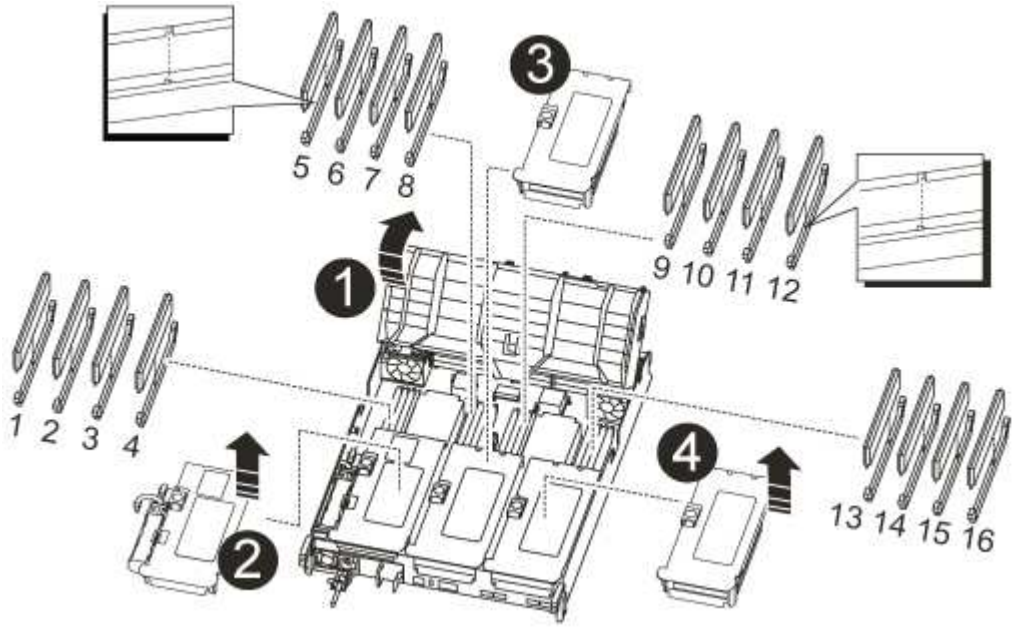


1	Air duct locking tabs
2	Risers
3	Air duct

Replace a DIMM

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

1. If you are not already grounded, properly ground yourself.
2. Remove the applicable riser.



1	Air duct cover
2	Riser 1 and DIMM bank 1-4
3	Riser 2 and DIMM bank 5-8 and 9-12
4	Riser 3 and DIMM 13-16

   - If you are removing or moving a DIMM in bank 1-4, unplug the NVRAM battery, unlock the locking latch on Riser 1, and then remove the riser.
   - If you are removing or moving a DIMM in bank 5-8 or 9-12, unlock the locking latch on Riser 2, and then remove the riser.
   - If you are removing or moving a DIMM in bank 13-16, unlock the locking latch on Riser 3, and then remove the riser.
3. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

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

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

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

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

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

7. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
8. Reinstall any risers that you removed from the controller module.

   If you removed the NVRAM riser, Riser 1, make sure that you plug the NVRAM battery into the controller module.

9. Close the air duct.

Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

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

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

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

3. Recable the system, as needed.

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

4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.

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

Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

Steps

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

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

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

Return the failed part to NetApp

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 - AFF A700s

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

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

Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.

- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

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

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

- Determine whether SED authentication is enabled.

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

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

About this task

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

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

Procedure

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

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

Option 1: Replace SSD

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

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

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

      You can enter the command on either controller module.

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

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

      You must disable automatic drive assignment on both controller modules.

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

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

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

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

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

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

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

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

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

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

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

      You can enter the command on either controller module.

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

      You can enter the command on either controller module.

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

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

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

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

Option 2: Replace HDD

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

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

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

      You can enter the command on either controller module.

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

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

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

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

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

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

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

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

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

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

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

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

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

       You can enter the command on either controller module.

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

       You can enter the command on either controller module.

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

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

       You must reenable automatic drive assignment on both controller modules.

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

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

Fan

Shut down the impaired controller - AFF A700s

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

About this task

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

Remove the controller module - AFF A700s

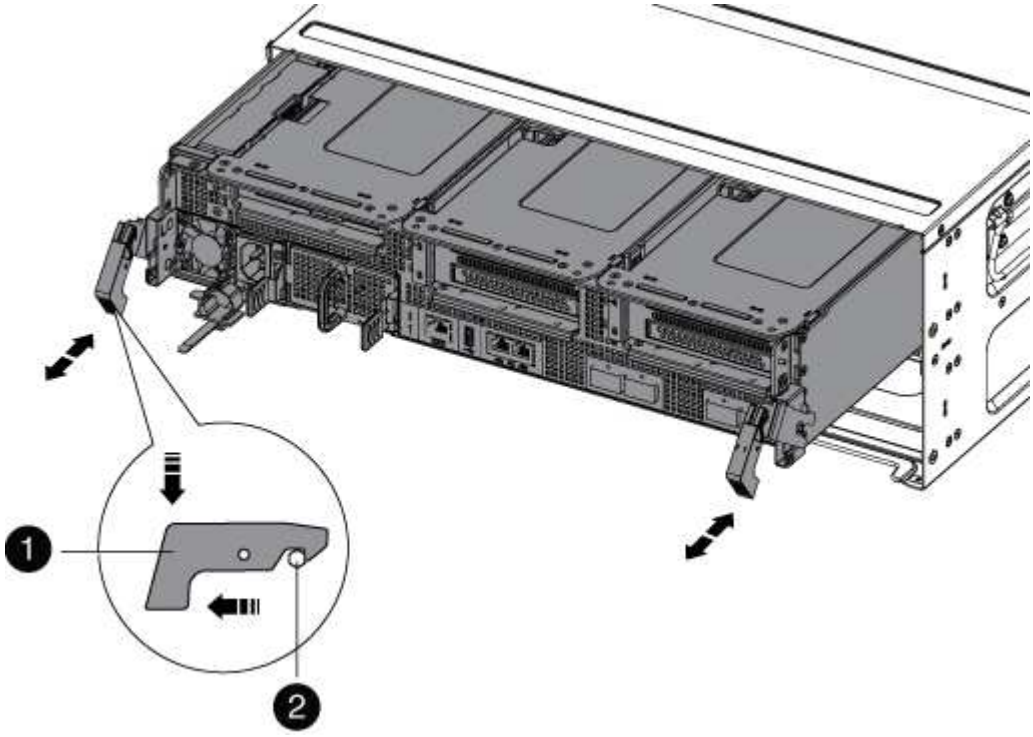
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

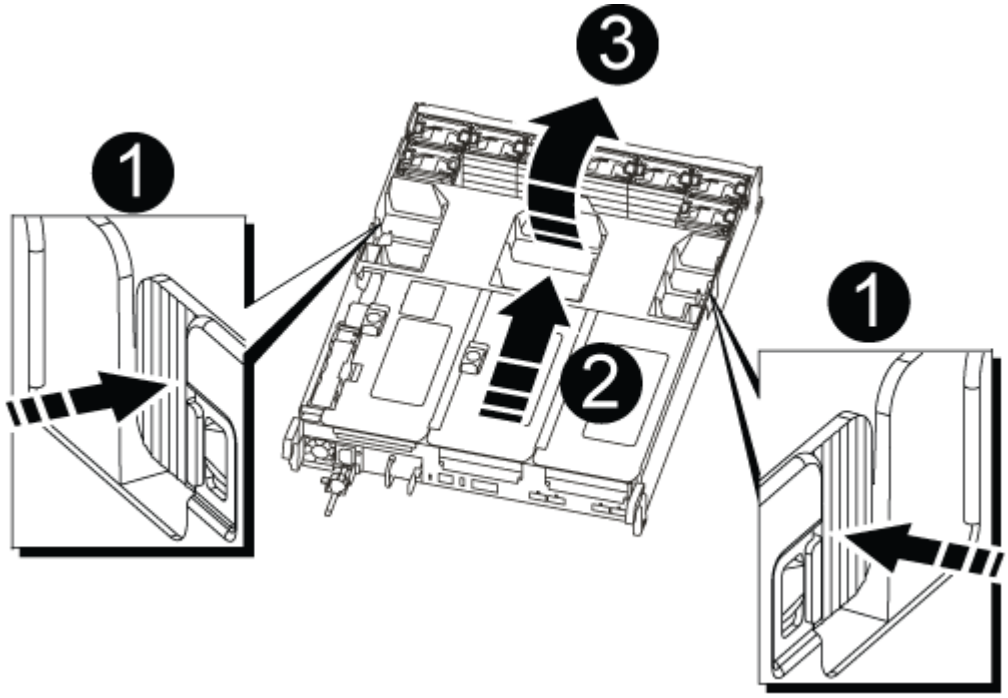


1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

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

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

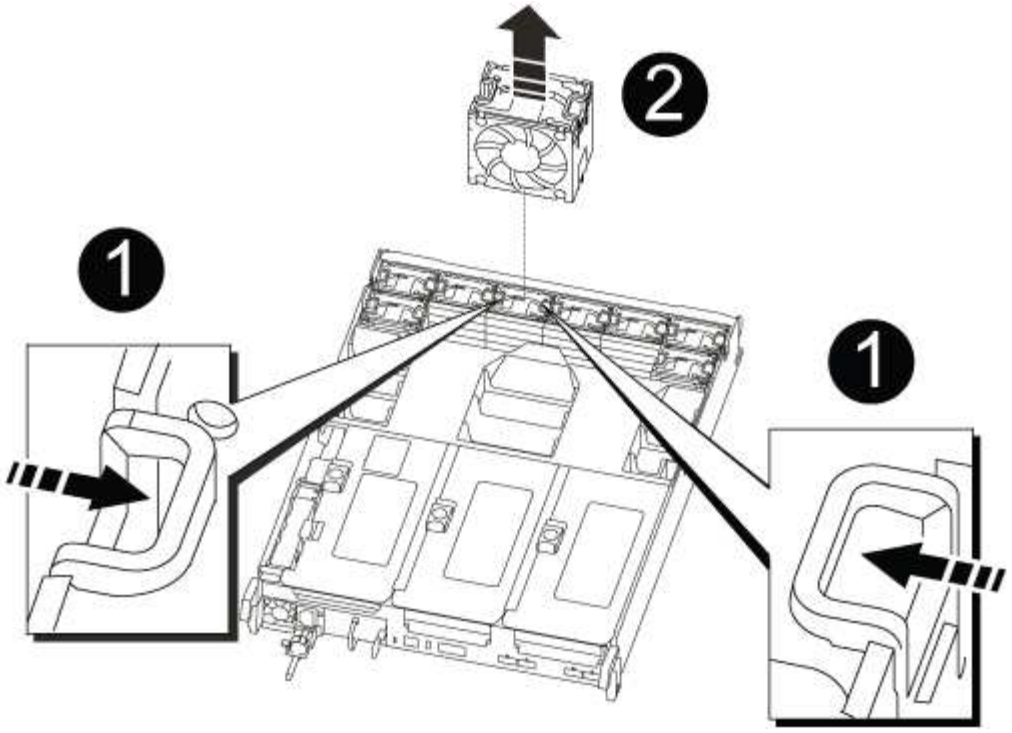


1	Air duct locking tabs
2	Risers
3	Air duct

Replacing a fan - AFF A700s

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

1. If you are not already grounded, properly ground yourself.
2. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
3. Remove the fan module by pinching the locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.



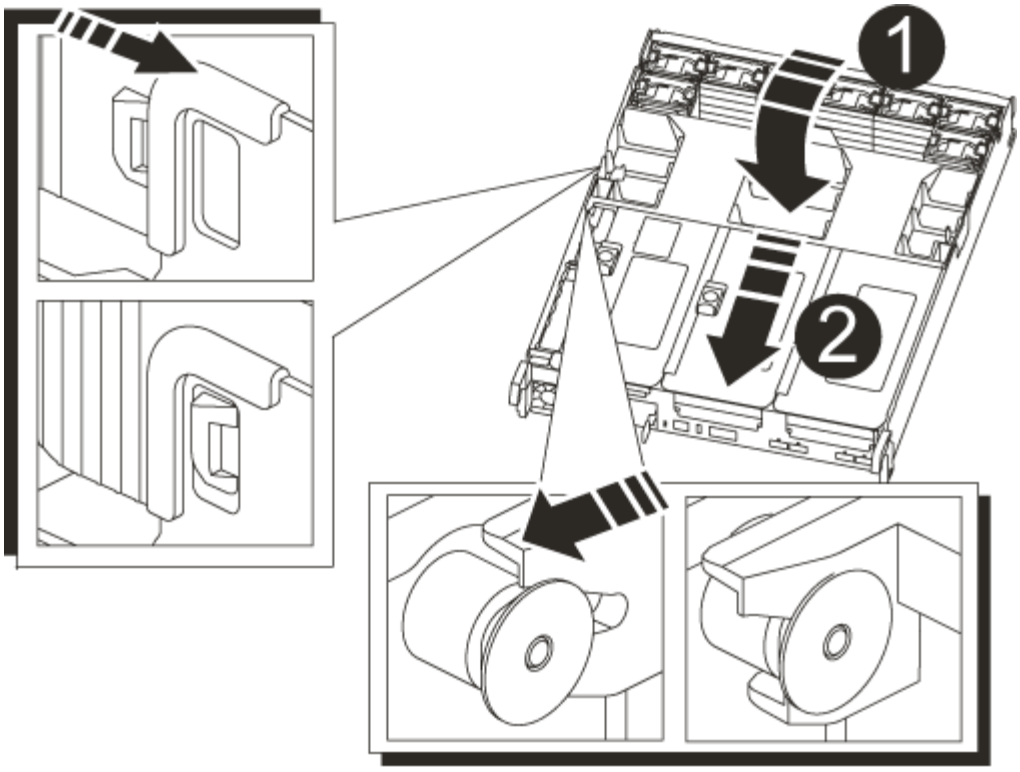
1	Fan locking tabs
2	Fan module

4. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module until the locking latches click into place.

Reinstall the controller module - AFF A700s

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

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Locking tabs
2	Slide plunger

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

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

4. Recable the system, as needed.

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

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

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

   Be sure to exit Maintenance mode after completing the conversion.

8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Return the failed part to NetApp - AFF A700s

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

Replace the NVRAM battery - AFF A700s

To replace an NVRAM battery in the system, you must remove the controller module from the system, remove the battery, replace the battery, and then reinstall the controller module.

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

Shut down the impaired controller

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

About this task

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

Steps

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

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

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

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

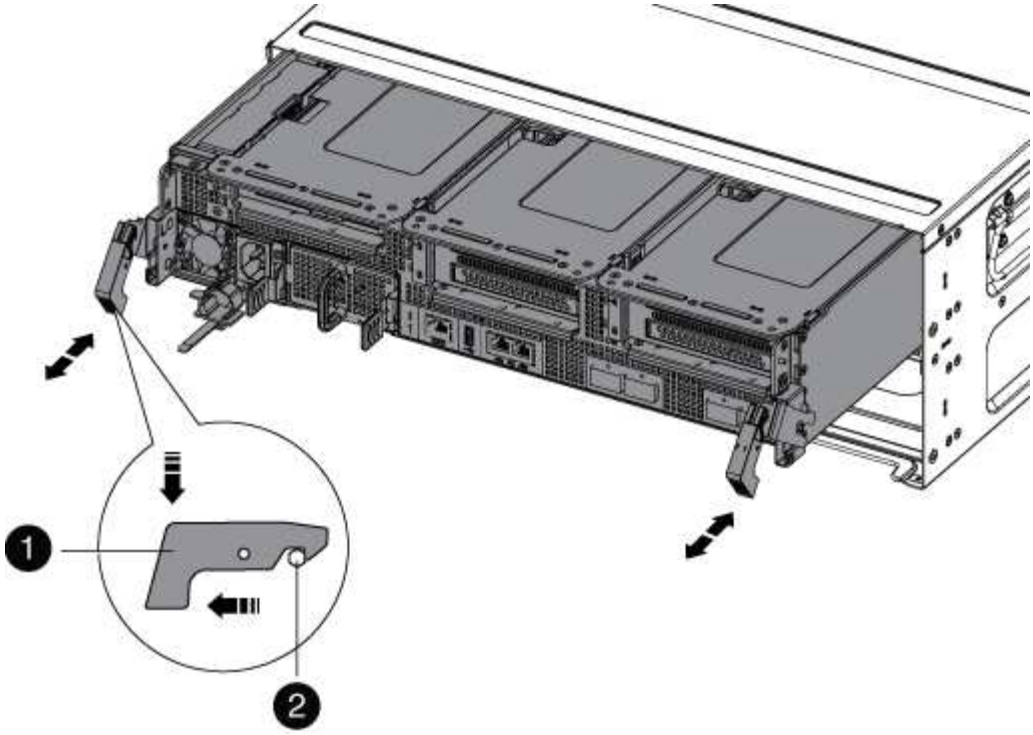
Remove the controller module

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

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

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.



1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

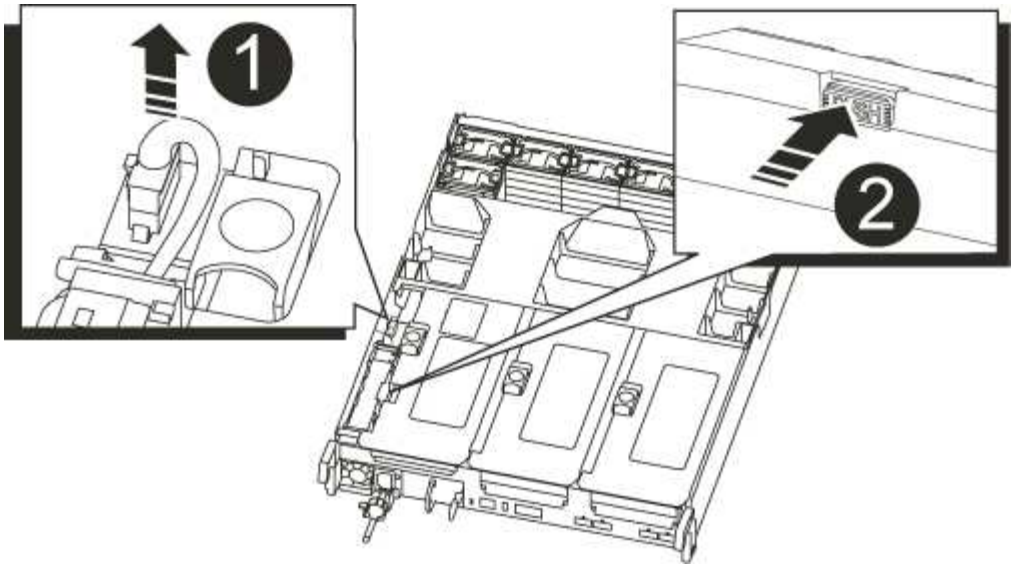
   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

7. Set the controller module aside in a safe place.

Replace the NVRAM battery

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

1. If you are not already grounded, properly ground yourself.
2. Locate the NVRAM battery on the left side of the riser module, Riser 1.



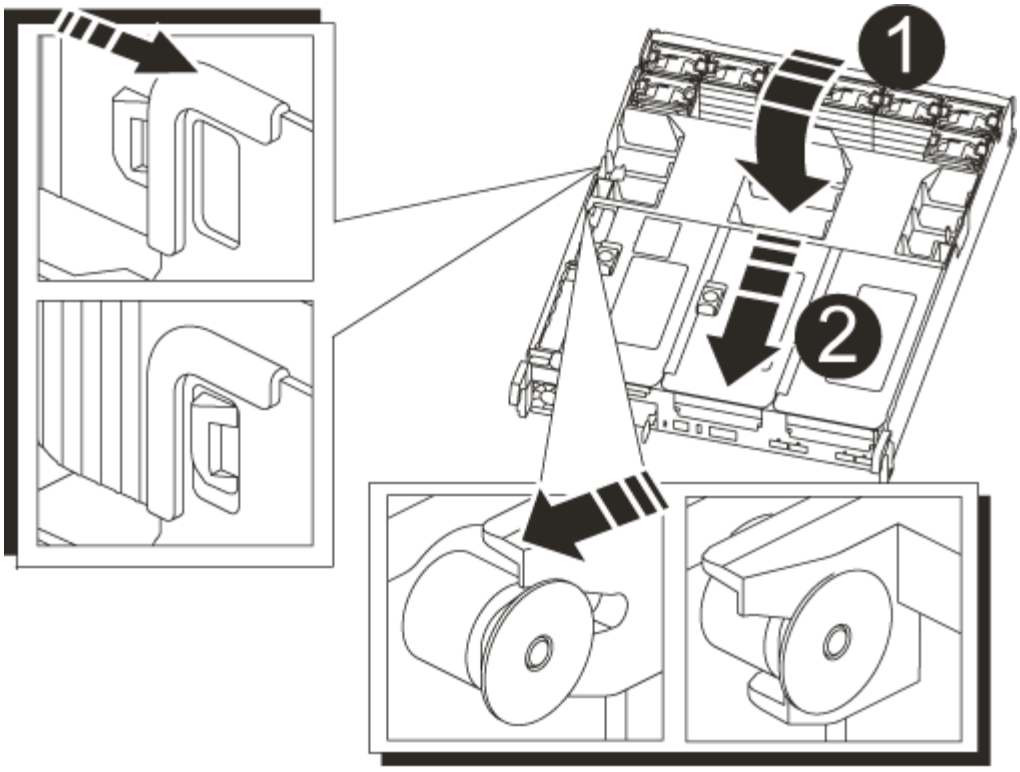
1	NVRAM battery plug
2	Blue NVRAM battery locking tab

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Push the blue locking tab on the battery holder, so that the latch releases from the holder.
5. Slide the battery down the riser bracket, lift the battery out of the controller, and then set it aside.
6. Slide the replacement battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and locks into place.
7. Plug the battery plug into the riser socket and make sure that the plug locks into place.

Reinstall the controller module

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

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Locking tabs
2	Slide plunger

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

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

4. Recable the system, as needed.

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

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

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

   Be sure to exit Maintenance mode after completing the conversion.

8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Return the failed part to NetApp

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

Replace the NVRAM module and NVRAM DIMMs - AFF A700s

To replace a failed NVRAM card, you must remove the NVRAM riser, Riser 1, from the controller module, remove the failed card from the riser, install the new NVRAM card in the riser, and then reinstall the riser in the controller module. Because the system ID is derived from the NVRAM card, if replacing the module, disks belonging to the system are reassigned to the new system ID.

Before you begin

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

Shut down the impaired controller

Steps

To shut down the impaired controller, you must determine the status of the controller and,

if necessary, take over the controller so that the healthy controller continues to serve data from the impaired controller storage.

About this task

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

     ONTAP 9 NetApp Encryption Power Guide

Remove the controller module

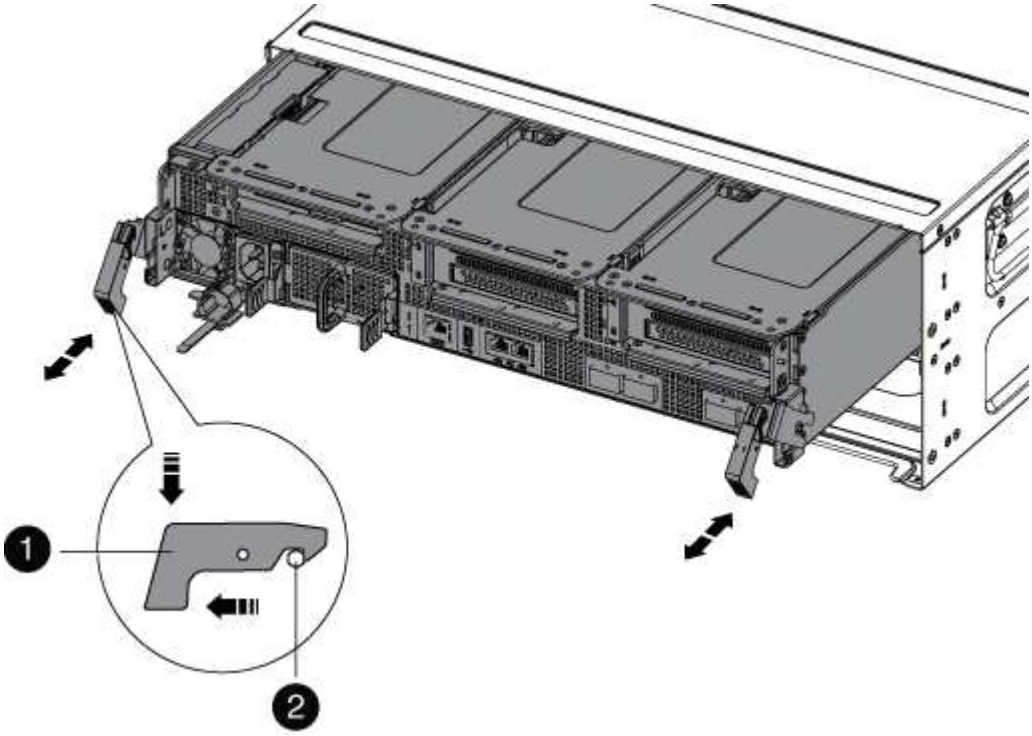
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

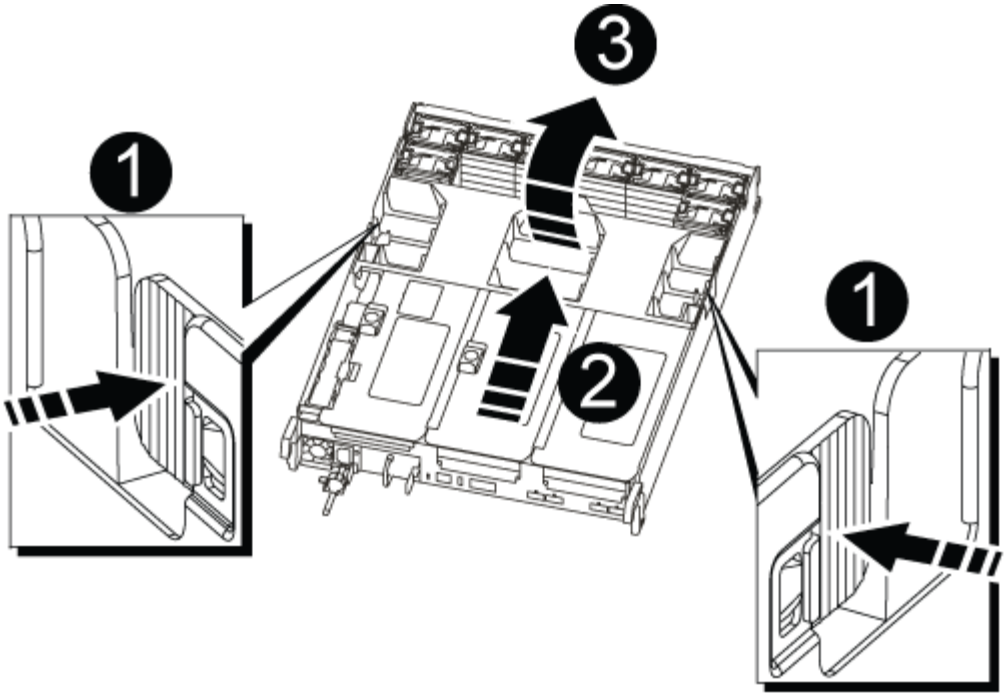


1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

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

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



1	Air duct locking tabs
2	Risers
3	Air duct

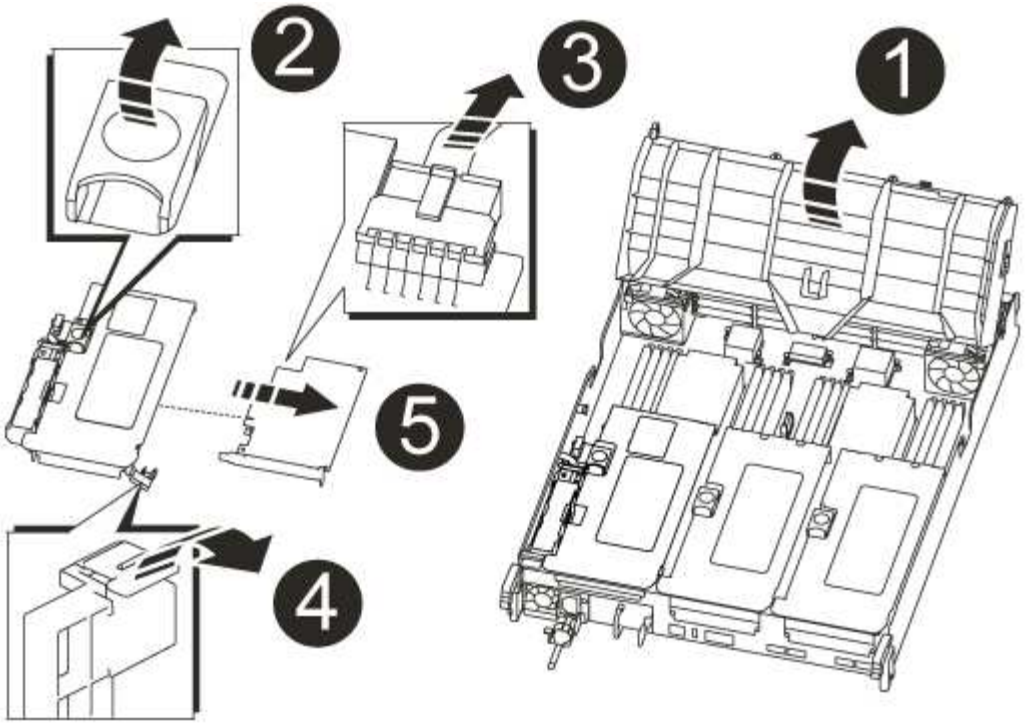
Remove the NVRAM card

Replacing the NVRAM consist of removing the NVRAM riser, Riser 1, from the controller module, disconnecting the NVRAM battery from the NVRAM card, removing the failed NVRAM card and installing the replacement NVRAM card, and then reinstalling the NVRAM riser back into the controller module.

1. If you are not already grounded, properly ground yourself.
2. Remove the NVRAM riser, Riser 1, from the controller module:
   a. Rotate the riser locking latch on the left side of the riser up and toward the fans.

      The NVRAM riser raises up slightly from the controller module.

   b. Lift the NVRAM riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser straight up out of the controller module, and then place it on a stable, flat surface so that you can access the NVRAM card.



1	Air duct
2	Riser 1 locking latch
3	NVRAM battery cable plug connecting to the NVRAM card
4	Card locking bracket
5	NVRAM card

3. Remove the NVRAM card from the riser module:
   a. Turn the riser module so that you can access the NVRAM card.
   b. Unplug the NVRAM battery cable that is attached to the NVRAM card.
   c. Press the locking bracket on the side of the NVRAM riser, and then rotate it to the open position.
   d. Remove the NVRAM card from the riser module.
4. Install the NVRAM card into the NVRAM riser:
   a. Align the card with the card guide on the riser module and the card socket in the riser.
   b. Slide the card squarely into the card socket.

      Make sure that the card is completely and squarely seated into the riser socket.

   c. Connect the battery cable to the socket on the NVRAM card.

d. Swing the locking latch into the locked position and make sure that it locks in place.

5. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
   c. Swing the locking latch down and click it into the locked position.

      When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

   d. Reinsert any SFP modules that were removed from the PCIe cards.

Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

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

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

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

3. Recable the system, as needed.

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

4. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

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

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

Verify the system ID change on an HA system

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

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

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

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

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

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

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

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

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

   d. Return to the admin privilege level: `set -privilege admin`
5. Give back the controller:

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

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

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

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

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

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

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

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

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

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

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

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

Restore Storage and Volume Encryption functionality

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

Step

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

Return the failed part to NetApp

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 PCIe card - AFF A700s

To replace a PCIe card, you must disconnect the cables from the cards in the riser, remove the riser, replace the riser, and then recable the cards in that riser.

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

Step 1: Shut down the impaired controller

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

About this task

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

Steps

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

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

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

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to Remove controller module.

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

Step 2: Remove the controller module

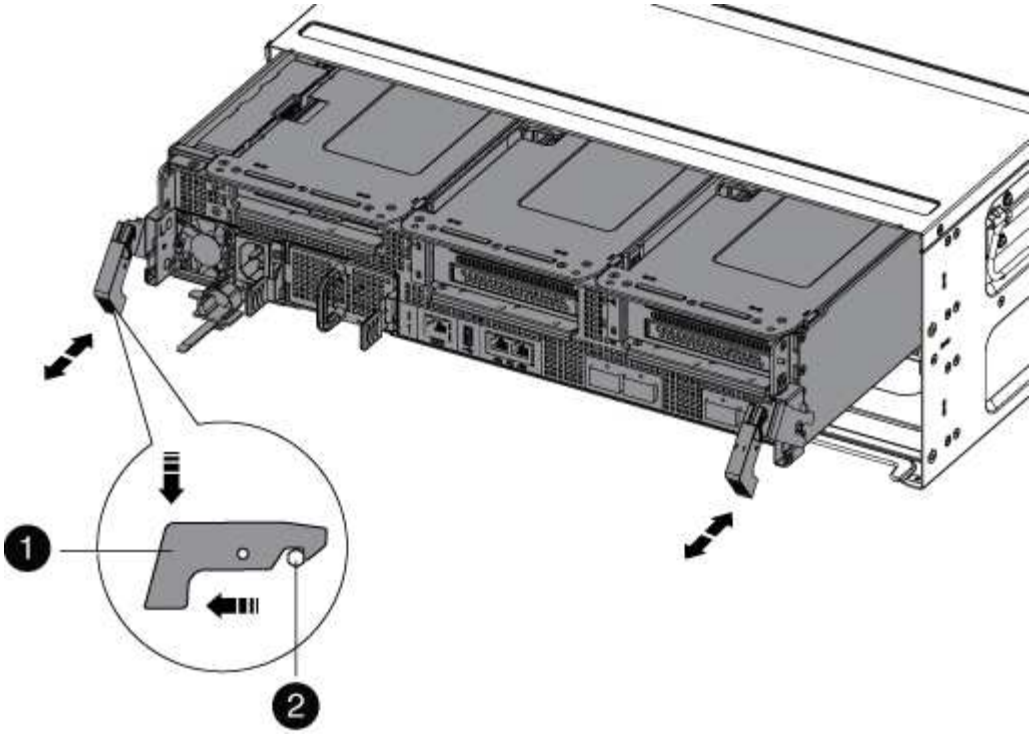
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

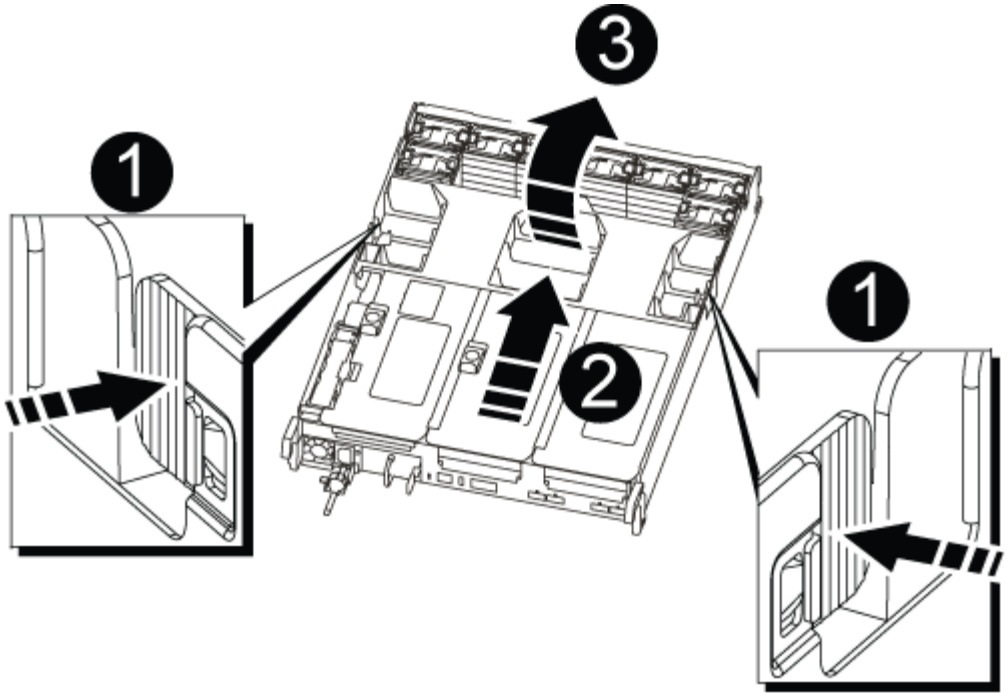


1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

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

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



+

1	Air duct locking tabs
2	Risers
3	Air duct

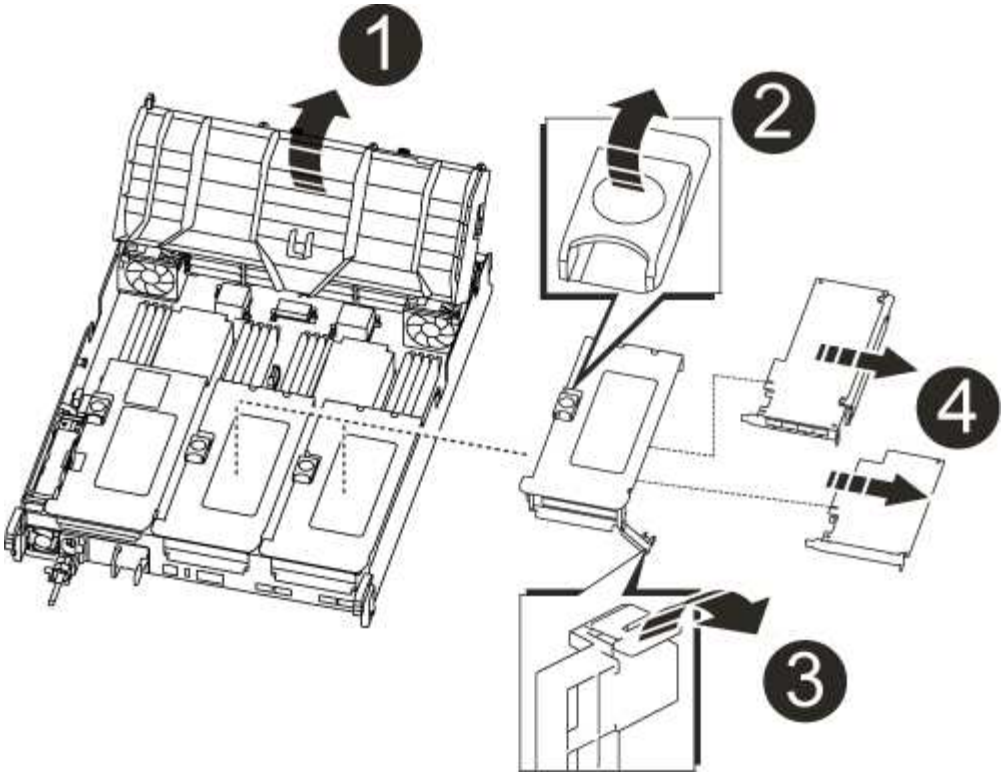
Step 3: Replace a PCIe card

To replace a PCIe card, you must remove the cabling and any SFPs from the ports on the PCIe cards in the target riser, remove the riser from the controller module, remove and replace the PCIe card, reinstall the riser, and recable it.

1. If you are not already grounded, properly ground yourself.
2. Remove the PCIe riser from the controller module:
   a. Remove any SFP modules that might be in the PCIe cards.
   b. Rotate the module locking latch on the left side of the riser up and toward the fan modules.

      The PCIe riser raises up slightly from the controller module.

   c. Lift the PCIe riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.



1	Air duct
2	Riser locking latch
3	Card locking bracket
4	Riser 2 (middle riser) and PCI cards in riser slots 2 and 3.

3. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
   c. Remove the PCIe card from the riser.
4. Install the PCIe card into the same slot in PCIe riser:
   a. Align the card with the card guide on the riser and the card socket in the riser, and then slide it squarely into the socket in the riser.

      Make sure that the card is completely and squarely seated into the riser socket.

   b. Swing the locking latch into place until it clicks into the locked position.
5. Install the riser into the controller module:
   a. Align the lip of the riser with the underside of the controller module sheet metal.
   b. Guide the riser along the pins in the controller module, and then lower the riser into the controller

module.

c. Swing the locking latch down and click it into the locked position.

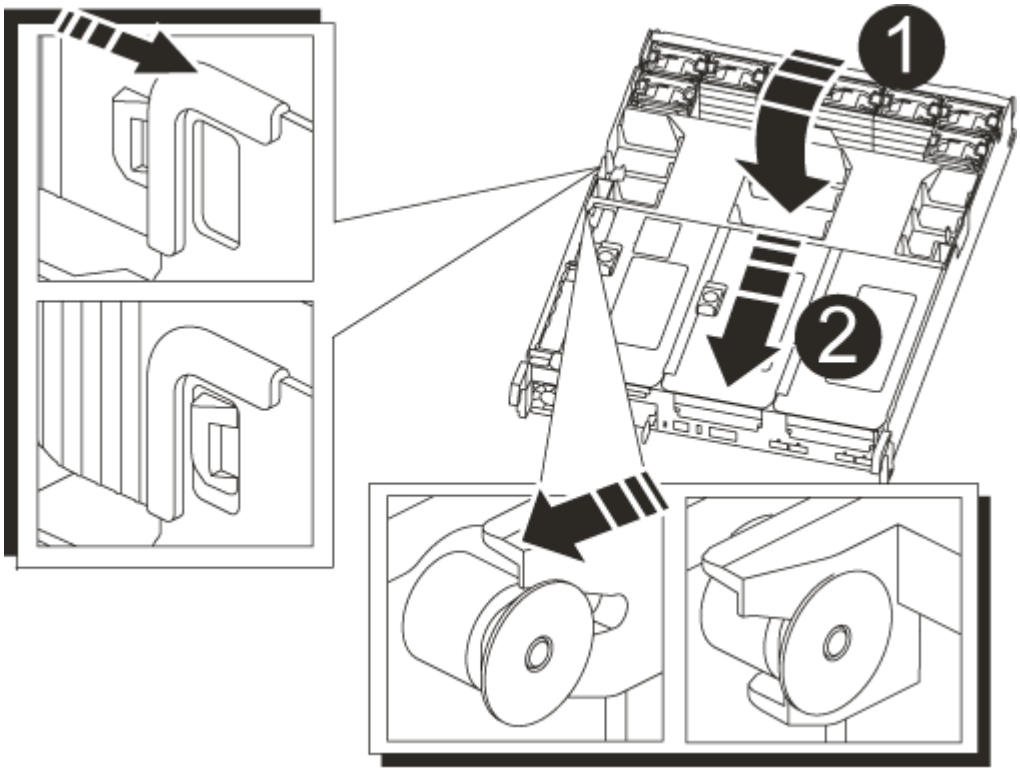
   When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

d. Reinsert any SFP modules that were removed from the PCIe cards.

Step 4: Reinstall the controller module

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

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, close the air duct:
   a. Swing the air duct all the way down to the controller module.
   b. Slide the air duct toward the risers until the locking tabs click into place.
   c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Locking tabs
2	Slide plunger

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

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

4. Recable the system, as needed.

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

5. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
6. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
7. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the nicadmin convert command from Maintenance mode.

   Be sure to exit Maintenance mode after completing the conversion.

8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 5: Return the failed part to NetApp

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

Swap out a power supply - AFF A700s

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

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

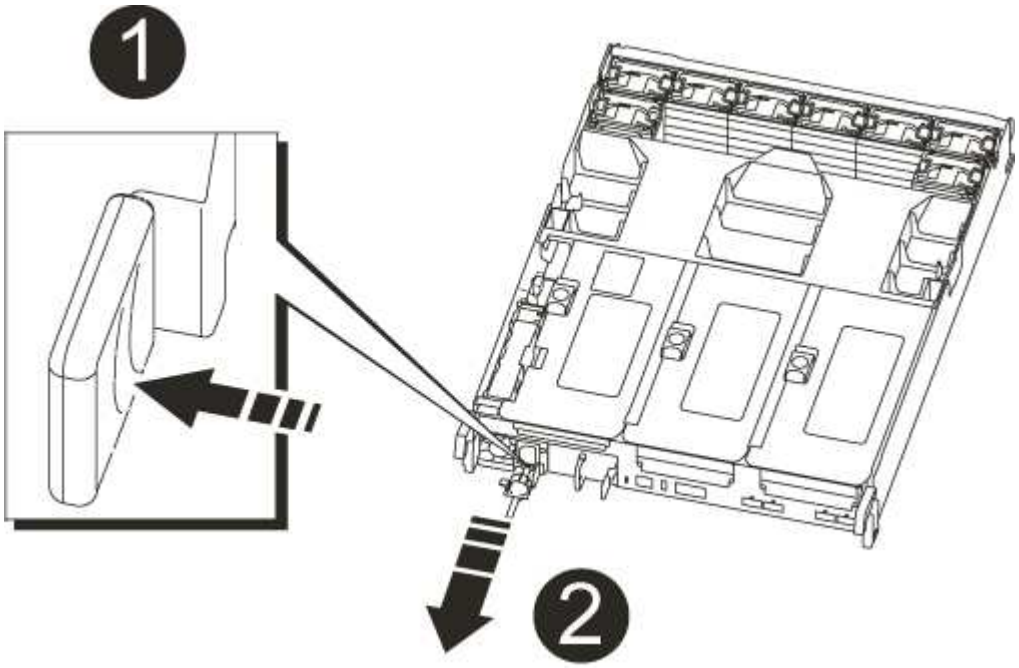
It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

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



1	Blue power supply locking tab
2	Power supply

5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into

place.

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

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

6. Close the cam handle by swinging it down as far as it will go.
7. Reconnect the power supply cabling:
   a. Reconnect the power cable to the power supply and the power source.
   b. Secure the power cable to the power supply using the power cable retainer.

   Once power is restored to the power supply, the status LED should be green.
8. 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 - AFF A700s

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

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

Shut down the impaired controller

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

About this task

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

Steps

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

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`
2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

Remove the controller module

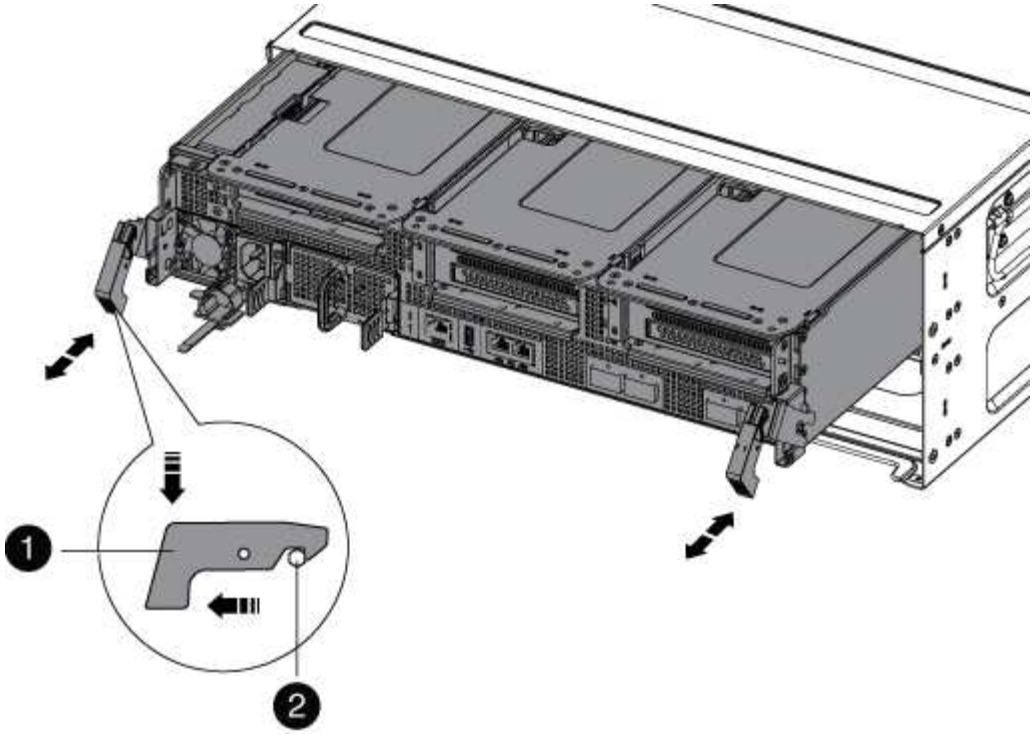
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.
4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

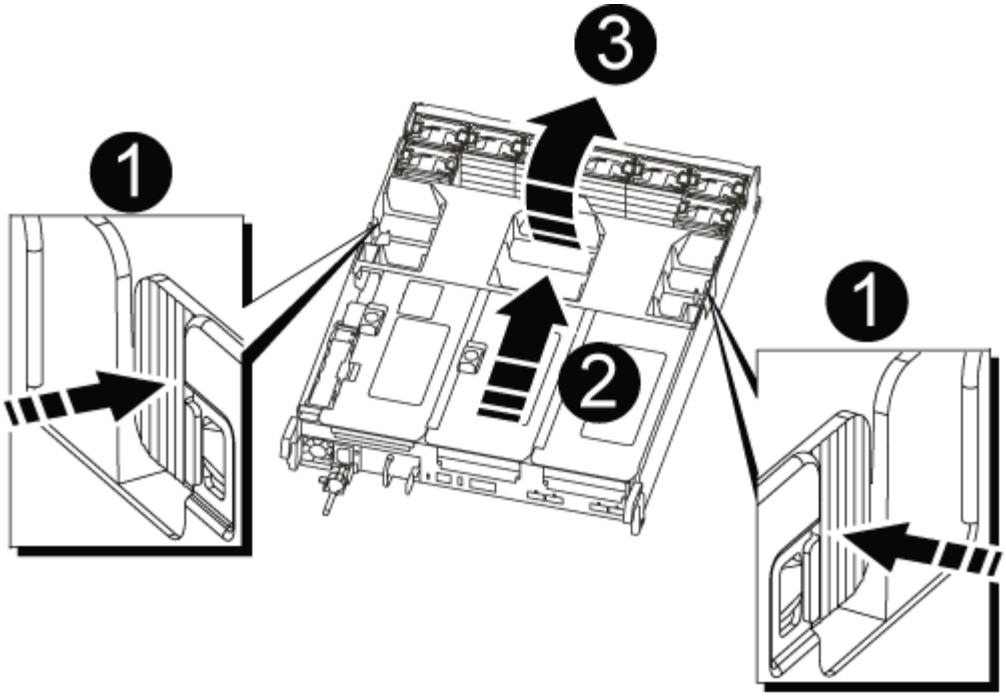


1	Locking latch
2	Locking pin

6. Slide the controller module out of the chassis.

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

7. Place the controller module on a stable, flat surface, and then open the air duct:
   a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
   b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

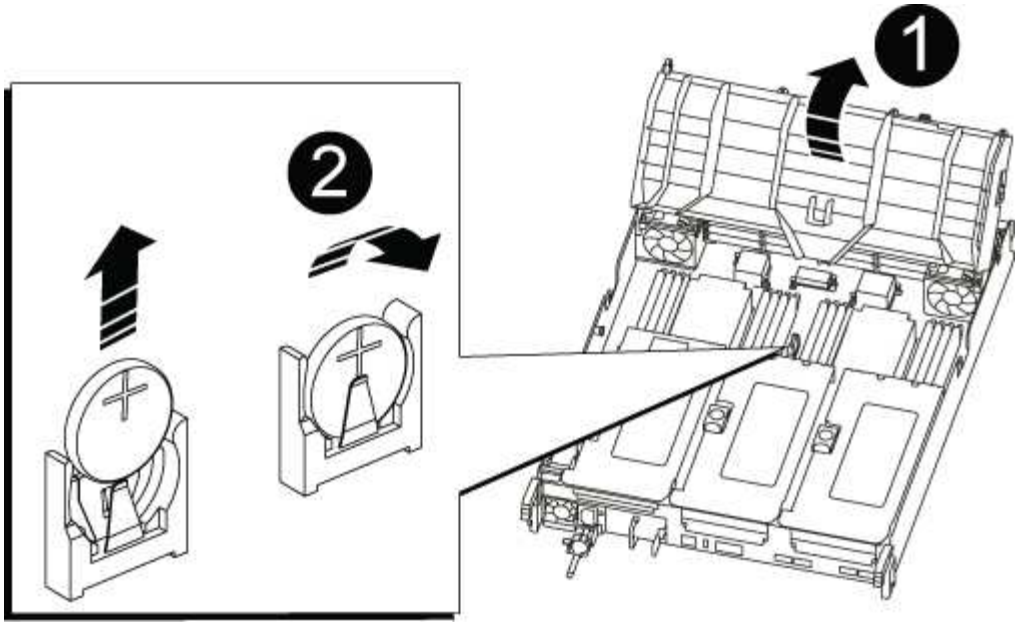


1	Air duct locking tabs
2	Risers
3	Air duct

Replace the RTC battery

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

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.



1	Air duct
2	RTC battery and housing

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

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

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

Reinstall the controller module and setting time/date after RTC battery replacement

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

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

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

3. Recable the system, as needed.

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

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:
   a. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

   b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, check the time and date.
   c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
   d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
   e. Confirm the date and time on the target controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Return the failed part to NetApp

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.

System-Level Diagnostics for AFF A700s

System-Level Diagnostics for AFF A700s is available outside this library. You will be prompted to log in using your NetApp Support Site credentials.

AFF A700s System-Level Diagnostics