NetApp

Maintain
ONTAP Systems

NetApp
August 11, 2022

Table of Contents

Maintain

Boot media

Overview of boot media replacement - AFF A700 and FAS9000

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

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

You also must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:

  - For nondisruptive replacement, the HA pair does not require connection to a network to restore the `var` file system. The HA pair in a single chassis has an internal e0S connection, which is used to transfer `var` config between them.

  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.

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

- It is important that you apply the commands in these steps on the correct node:

  - The *impaired* node is the node on which you are performing maintenance.

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

Check onboard encryption keys

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

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

Steps

1. Check the status of the impaired controller:

   - If the impaired controller is at the login prompt, log in as `admin`.

   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.

   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact [mysupport.netapp.com](#).

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

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

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

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:

   ◦ If <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: Check 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: Check NVE or NSE on systems running ONTAP 9.6 and later.

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

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

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

Steps

1. Connect the console cable to the impaired controller.

2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

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

3. Check whether NSE is configured: `storage encryption disk show`

   ◦ If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.

   ◦ If NVE and NSE are not configured, it's safe to shut down the impaired controller.

Verify NVE configuration

Steps

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

   ◦ If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.

   ◦ If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.

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

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

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

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

   c. Shut down the impaired controller.

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

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

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

      ▪ Enter the command to display the OKM backup information: `security key-manager backup show`

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

      ▪ Return to admin mode: `set -priv admin`

      ▪ Shut down the impaired controller.

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

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

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

      ▪ Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`

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

      ▪ Enter the command to display the OKM backup information: `security key-manager backup show`

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

      ▪ Return to admin mode: `set -priv admin`

      ▪ You can safely shutdown the controller.

Verify NSE configuration

Steps

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

- If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.

- If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.

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

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

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

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

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

   c. Shut down the impaired controller.

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

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

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

      - Enter the command to display the OKM backup information: `security key-manager backup show`

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

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

      - Shut down the impaired controller.

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

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

        (i) 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`

        (i) 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`

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

    ◦ If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.

    ◦ If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.

    ◦ If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

    ◦ If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

2. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

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

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

    c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster

scenarios where you might need to manually recover OKM.

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

    e. Shut down the impaired controller.

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

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

    If the command fails, contact NetApp Support.

    mysupport.netapp.com

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

    c. Shut down the impaired controller.

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

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

> (i) 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`

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

    ◦ If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.

    ◦ If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

2. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

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

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

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

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

    e. You can safely shut down the controller.

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

    a. 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.

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

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

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

    mysupport.netapp.com

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

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

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

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

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

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

    h. You can safely shut down the controller.

Shut down the impaired controller - AFF A700 and FAS9000

Option 1: Most systems

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node. NOTE: Do not use this procedure if your system is in a two-node MetroCluster configuration.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

Option 3: Controller is in a two-node MetroCluster

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

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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the Administration overview with the CLI.
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

Replace the boot media - AFF A700 and FAS9000

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

Step 1: Remove the controller

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

❶	Cam handle release button
❷	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

❶	Controller module cover locking button

Step 2: Replace the boot media

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

1	Press release tab
2	Boot media

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

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

2. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.

3. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

5. Reinstall the controller module lid by aligning the pins on the lid with the slots on the motherboard carrier, and then slide the lid into place.

Step 3: Transfer the boot image to the boot media

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

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

- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.

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

Steps

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

2. Recable the controller module, as needed.

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

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

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

handle to the closed position.

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

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

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

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

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

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

   ◦ If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`

      ▪ filer_addr is the IP address of the storage system.

      ▪ netmask is the network mask of the management network that is connected to the HA partner.

      ▪ gateway is the gateway for the network.

      ▪ dns_addr is the IP address of a name server on your network.

      ▪ dns_domain is the Domain Name System (DNS) domain name.

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

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

7. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:

   a. Boot to Maintenance mode: `boot_ontap maint`

   b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t initiator adapter_name`

   c. Halt to return to Maintenance mode: `halt`

   The changes will be implemented when the system is booted.

Boot the recovery image - AFF A700 and FAS9000

The procedure for booting the impaired node from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1 Boot the recovery image in most systems

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

the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

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

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.

3. Restore the `var` file system:

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

If your system has…	Then…
No network connection and is in a MetroCluster IP configuration	a. Press `n` when prompted to restore the backup configuration.
	b. Reboot the system when prompted by the system.
	c. Wait for the iSCSI storage connections to connect.
	You can proceed after you see the following messages:

```
date-and-time [node-
name:iscsi.session.stateChanged:notice]:
iSCSI session state is changed to Connected
for the target iSCSI-target (type:
dr_auxiliary, address: ip-address).
date-and-time [node-
name:iscsi.session.stateChanged:notice]:
iSCSI session state is changed to Connected
for the target iSCSI-target (type:
dr_partner, address: ip-address).
date-and-time [node-
name:iscsi.session.stateChanged:notice]:
iSCSI session state is changed to Connected
for the target iSCSI-target (type:
dr_auxiliary, address: ip-address).
date-and-time [node-
name:iscsi.session.stateChanged:notice]:
iSCSI session state is changed to Connected
for the target iSCSI-target (type:
dr_partner, address: ip-address).
```

d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.

If you are prompted to continue with the update, press `y`.

4. Ensure that the environmental variables are set as expected:

   a. Take the node to the LOADER prompt.

   b. Check the environment variable settings with the `printenv` command.

   c. If an environment variable is not set as expected, modify it with the `setenv environment-variable-name changed-value` command.

   d. Save your changes using the `savenv` command.

5. The next depends on your system configuration:

   ◦ If your system has onboard keymanager, NSE or NVE configured, go to Restore OKM, NSE, and NVE as needed

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

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

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

7. Connect the console cable to the partner node.

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

9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

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

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

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

Option 2: Boot the recovery image in a two-node MetroCluster configuration

You must boot the ONTAP image from the USB drive and verify the environmental variables.

This procedure applies to systems in a two-node MetroCluster configuration.

Steps

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

   The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.

3. After the image is installed, start the restoration process:

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

   b. Press `y` when prompted to reboot to start using the newly installed software.

      You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.

5. Verify that the environmental variables are set as expected.

   a. Take the node to the LOADER prompt.

b. Check the environment variable settings with the `printenv` command.

c. If an environment variable is not set as expected, modify it with the `setenv` *environment-variable-name changed-value* command.

d. Save your changes using the `savenv` command.

e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF A700 and FAS9000

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- -------------- -------------- ---------
-------------------
1     cluster_A
            controller_A_1 configured     enabled   heal roots
completed
      cluster_B
            controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster                 Configuration State     Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster                 Configuration State     Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore OKM, NSE, and NVE as needed - AFF A700 and FAS9000

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

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

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

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

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

Steps

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

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

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.

5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.

6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

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

Example of backup data:

```
--------------------------BEGIN BACKUP--------------------------
TmV0QXBwlEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOlyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAIAAAAAAgAZJElWvdeHr5RCAvHGclo+wAAAAAAAAA
lgAAAAAAAoAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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.

  (i) | 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.

       (i) | 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.

       (i) | 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.

   > (i) 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 A700 and FAS9000

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 caching module or add/replace a core dump module - AFF A700 and FAS9000

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation. If AutoSupport is not enabled, you can locate the failed caching module by the fault LED on the front of the module. You can also add or replace the 1TB, X9170A core dump module, which is required if you are installing NS224 drive shelves in an AFF A700 system.

Before you begin

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

- For instructions about hot swapping the caching module, see Hot-swapping a caching module.

- When removing, replacing, or adding caching or core dump modules, the target node must be halted to the LOADER.

- AFF A700 supports the 1TB core dump module, X9170A, which is required if you are adding NS224 drive shelves.

- The core dump modules can be installed in slots 6-1 and 6-2. The recommended best practice is to install the module in slot 6-1.

- The X9170A core dump module is not hot-swappable.

Step 1: Shutting down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

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

About this task

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
       State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
      Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
-----------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
      Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace or add a caching module

The NVMe SSD Flash Cache modules (FlashCache or caching modules) are separate modules. They are located in the front of the NVRAM module. To replace or add a caching module, locate it on the rear of the system on slot 6, and then follow the specific sequence of steps to replace it.

Before you begin

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

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The target node must be at the LOADER prompt before adding or replacing the caching module.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

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

2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.

3. Remove the caching module:

   ⓘ If you are adding another caching module to your system, remove the blank module and go to the next step.

1	Orange release button.
2	Caching module cam handle.

a. Press the orange release button on the front of the caching module.

> ⓘ Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

Be sure to support the caching module as you remove it from the NVRAM10 module.

4. Install the caching module:

a. Align the edges of the caching module with the opening in the NVRAM10 module.

b. Gently push the caching module into the bay until the cam handle engages.

c. Rotate the cam handle until it locks into place.

Step 3: Add or replace an X9170A core dump module

The 1TB cache core dump, X9170A, is only used in the AFF A700 systems. The core dump module cannot be hot-swapped. The core dump module typically is located in the

front of the NVRAM module in slot 6-1 in the rear of the system. To replace or add the core dump module, locate slot 6-1, and then follow the specific sequence of steps to add or replace it.

Before you begin

- Your system must be running ONTAP 9.8 or later in order to add a core dump module.

- The X9170A core dump module is not hot-swappable.

- The target node must be at the LOADER prompt before adding or replacing the code dump module.

- You must have received two X9170 core dump modules; one for each controller.

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

Steps

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

2. If you are replacing a failed core dump module, locate and remove it:

❶	Orange release button.
❷	Core dump module cam handle.

    a. Locate the failed module by the amber Attention LED on the front of the module.

    b. Press the orange release button on the front of the core dump module.

| | Do not use the numbered and lettered I/O cam latch to eject the core dump module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the core dump module. |

c. Rotate the cam handle until the core dump module begins to slide out of the NVRAM10 module.

d. Gently pull the cam handle straight toward you to remove the core dump module from the NVRAM10 module and set it aside.

Be sure to support the core dump module as you remove it from the NVRAM10 module.

3. Install the core dump module:

a. If you are installing a new core dump module, remove the blank module from slot 6-1.

b. Align the edges of the core dump module with the opening in the NVRAM10 module.

c. Gently push the core dump module into the bay until the cam handle engages.

d. Rotate the cam handle until it locks into place.

Step 4: Reboot the controller after FRU replacement

After you replace the FRU, you must reboot the controller module.

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- --------------      --------------  ---------
--------------------
1     cluster_A
            controller_A_1 configured     enabled    heal roots
completed
      cluster_B
            controller_B_1 configured     enabled    waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster                  Configuration State     Mode
--------------------     -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster                  Configuration State     Mode
--------------------     -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

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.

Hot-swap a caching module - AFF A700 and FAS9000

The NVMe SSD FlashCache modules (FlashCache or caching modules) are located in the front of the NVRAM10 module in Slot 6 of FAS9000 systems only. Beginning with ONTAP 9.4, you can hot-swap the caching module of the same capacity from the same or different supported vendor.

Before you begin

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

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

Steps

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

2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.

3. Prepare the caching module slot for replacement as follows:

   a. For ONTAP 9.7 and earlier:

      i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

      ii. In admin privilege level, prepare the target NVMe slot for replacement, responding `y` when prompted whether to continue: `system controller slot module replace -node node_name -slot slot_number` The following command prepares slot 6-2 on node1 for replacement, and displays a message that it is safe to replace:

```
::> system controller slot module replace -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node node1 will be powered
off for replacement.
Do you want to continue? (y|n): `y`

The module has been successfully powered off.  It can now be
safely replaced.
After the replacement module is inserted, use the "system
controller slot module insert" command to place the module into
service.
```

   iii. Display the slot status with the system controller slot module show command.

      The NVMe slot status displays waiting-for-replacement in the screen output for the caching module that needs replacing.

  b. For ONTAP 9.8 and later:

    i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

    ii. In admin privilege level, prepare the target NVMe slot for removal, responding `y` when prompted whether to continue: `system controller slot module remove -node node_name -slot slot_number` The following command prepares slot 6-2 on node1 for removal, and displays a message that it is safe to remove:

```
::> system controller slot module remove -node node1 -slot 6-2

Warning: SSD module in slot 6-2 of the node node1 will be powered
off for removal.
Do you want to continue? (y|n): `y`

The module has been successfully removed from service and powered
off. It can now be safely removed.
```

    iii. Display the slot status with the `system controller slot module show` command.

      The NVMe slot status displays `powered-off` in the screen output for the caching module that needs replacing.

    (i)   See the Command man pages for your version of ONTAP for more details.

4. Remove the caching module:

❶	Orange release button.
❷	Caching module cam handle.

   a. Press the orange release button on the front of the caching module.

> ⓘ Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

   b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

   c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

     Be sure to support the caching module as you remove it from the NVRAM10 module.

5. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM10 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

6. Bring the replacement caching module online by using the `system controller slot module insert` command as follows:

   The following command prepares slot 6-2 on node1 for power-on, and displays a message that it is

powered on:

```
::> system controller slot module insert -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node localhost will be powered
on and initialized.
Do you want to continue? (y|n): `y`

The module has been successfully powered on, initialized and placed into
service.
```

7. Verify the slot status using the `system controller slot module show` command.

   Make sure that command output reports status for slot 6-1 or 6-2 as `powered-on` and ready for operation.

8. Verify that the replacement caching module is online and recognized, and then visually confirm that the amber attention LED is not lit: `sysconfig -av slot_number`

   (i) If you replace the caching module with a caching module from a different vendor, the new vendor name is displayed in the command output.

9. 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 A700 and FAS9000

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

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A700 and FAS9000

To replace the chassis, you must shutdown the controllers.

Option 1: Shut down the controllers

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

About this task

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

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

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

Steps

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

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

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

   The confirmation message looks like the following:

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

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

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

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

   Answer `y` when prompted.

Option 2: Shut down a node in a two-node MetroCluster configuration

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
   Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
    Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes          RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online        0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Move and replace hardware - AFF A700 and FAS9000

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

Step 1: Remove the power supplies

Steps

Removing the power supplies when replacing a chassis involves turning off, disconnecting, and then removing the power supply from the old chassis.

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

2. Turn off the power supply and disconnect the power cables:

    a. Turn off the power switch on the power supply.

    b. Open the power cable retainer, and then unplug the power cable from the power supply.

    c. Unplug the power cable from the power source.

3. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.

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

❶	Locking button

4. Repeat the preceding steps for any remaining power supplies.
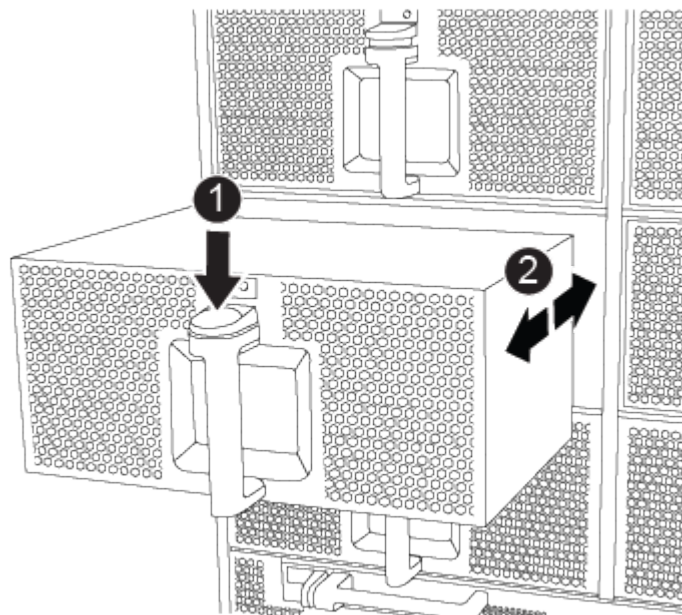
Step 2: Remove the fans

To remove the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

Steps

1. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.

2. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

| ⚠ | The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you. |

1	Orange release button

3. Set the fan module aside.

4. Repeat the preceding steps for any remaining fan modules.

Step 3: Remove the controller module

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

Steps

1. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.

2. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button
2	Cam handle

3. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

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

Step 4: Remove the I/O modules

Steps

To remove I/O modules from the old chassis, including the NVRAM modules, follow the specific sequence of steps. You do not have to remove the FlashCache module from the NVRAM module when moving it to a new chassis.

1. Unplug any cabling associated with the target I/O module.

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

2. Remove the target I/O module from the chassis:

   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

❶	Lettered and numbered I/O cam latch
❷	I/O cam latch completely unlocked

3. Set the I/O module aside.
4. Repeat the preceding step for the remaining I/O modules in the old chassis.

Step 5: Remove the De-stage Controller Power Module

Steps

You must remove the de-stage controller power modules from the old chassis in preparation for installing the replacement chassis.

1. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.

①	DCPM module orange locking button

2. Set the DCPM module aside in a safe place and repeat this step for the remaining DCPM module.

Step 6: Replace a chassis from within the equipment rack or system cabinet

Steps

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

1. Remove the screws from the chassis mount points.

   ⓘ   If the system is in a system cabinet, you might need to remove the rear tie-down bracket.

2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or *L* brackets in an equipment rack, and then set it aside.

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

4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or *L* brackets in an equipment rack.

5. Slide the chassis all the way into the equipment rack or system cabinet.

6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.

7. Secure the rear of the chassis to the equipment rack or system cabinet.

8. If you are using the cable management brackets, remove them from the old chassis, and then install them on the replacement chassis.

9. If you have not already done so, install the bezel.

Step 7: Move the USB LED module to the new chassis

Steps

Once the new chassis is installed into the rack or cabinet, you must move the USB LED module from the old chassis to the new chassis.

1. Locate the USB LED module on the front of the old chassis, directly under the power supply bays.

2. Press the black locking button on the right side of the module to release the module from the chassis, and then slide it out of the old chassis.

3. Align the edges of the module with the USB LED bay at the bottom-front of the replacement chassis, and gently push the module all the way into the chassis until it clicks into place.

Step 8: Install the de-stage controller power module when replacing the chassis

Steps

Once the replacement chassis is installed into the rack or system cabinet, you must reinstall the de-stage controller power modules into it.

1. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.

   > ⓘ The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

2. Repeat this step for the remaining DCPM module.

Step 9: Install fans into the chassis

Steps

To install the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

1. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

   When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

2. Repeat these steps for the remaining fan modules.

3. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Step 10: Install I/O modules

Steps

To install I/O modules, including the NVRAM/FlashCache modules from the old chassis, follow the specific sequence of steps.

You must have the chassis installed so that you can install the I/O modules into the corresponding slots in the new chassis.

1. After the replacement chassis is installed in the rack or cabinet, install the I/O modules into their corresponding slots in the replacement chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage, and then push the I/O cam latch all the way up to lock the module in place.

2. Recable the I/O module, as needed.

3. Repeat the preceding step for the remaining I/O modules that you set aside.

   > (i)   If the old chassis has blank I/O panels, move them to the replacement chassis at this time.

Step 11: Install the power supplies

Steps

Installing the power supplies when replacing a chassis involves installing the power supplies into the replacement chassis, and connecting to the power source.

1. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

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

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

2. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

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

3. Repeat the preceding steps for any remaining power supplies.

Step 12: Install the controller

Steps

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

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

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

2. Recable the console to the controller module, and then reconnect the management port.

3. Connect the power supplies to different power sources, and then turn them on.

4. With the cam handle in the open position, slide the controller module into the chassis and firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle until it clicks into the locked position.

> (i) Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.

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

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

6. Boot each node to Maintenance mode:

   a. As each node starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.

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

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

Complete the restoration and replacement process - AFF A700 and FAS9000

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

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

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

Steps

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

   The HA state should be the same for all components.

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

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

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

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

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

3. If you have not already done so, recable the rest of your system.

4. Exit Maintenance mode: `halt`

   The LOADER prompt appears.

Step 2: Running system-level diagnostics

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

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

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

Steps

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:

   a. Select the Maintenance mode option from the displayed menu.

   b. After the node boots to Maintenance mode, halt the node: `halt`

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

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

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

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

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

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

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

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

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

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

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

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

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

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: ``` SLDIAG: No log messages are present. ``` c. Exit Maintenance mode on both controllers: `halt` The system displays the LOADER prompt. (i) You must exit Maintenance mode on both controllers before proceeding any further. d. Enter the following command on both controllers at the LOADER prompt: `bye` e. Return the node to normal operation:
With two nodes in the cluster	Issue these commands: `node::> cluster ha modify -configured true` `node::> storage failover modify -node node0 -enabled true`
With more than two nodes in the cluster	Issue this command:`node::> storage failover modify -node node0 -enabled true`
In a two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.

If the system-level diagnostics tests…	Then…
Resulted in some test failures	Determine the cause of the problem. a. Exit Maintenance mode: `halt` b. Perform a clean shutdown, and then disconnect the power supplies. c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. d. Reconnect the power supplies, and then power on the storage system. e. Rerun the system-level diagnostics test.

Step 3: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
            controller_A_1 configured     enabled   heal roots
completed
      cluster_B
            controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

   ```
   cluster_B::> metrocluster show
   Cluster                 Configuration State     Mode
   --------------------    ------------------      ---------
    Local: cluster_B configured        switchover
   Remote: cluster_A configured        waiting-for-switchback
   ```

   The switchback operation is complete when the clusters are in the `normal` state.:

   ```
   cluster_B::> metrocluster show
   Cluster                 Configuration State     Mode
   --------------------    ------------------      ---------
    Local: cluster_B configured           normal
   Remote: cluster_A configured           normal
   ```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

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 module

Overview of controller module replacement - AFF A700 and FAS9000

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

- All drive shelves must be working properly.

- If your system is a FlexArray system or has a V_StorageAttach license, you must refer to the additional required steps before performing this procedure.

- If your system is in an HA pair, the healthy node must be able to take over the node that is being replaced (referred to in this procedure as the "impaired node").

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

  If this is the procedure you should use, note that the controller replacement procedure for a node in a four

or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

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

- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.

- You cannot change any drives or drive shelves as part of this procedure.

- In this procedure, the boot device is moved from the impaired node to the *replacement* node so that the *replacement* node will boot up in the same version of ONTAP as the old controller module.

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

  - The *impaired* node is the node that is being replaced.

  - The *replacement* node is the new node that is replacing the impaired node.

  - The *healthy* node is the surviving node.

- You must always capture the node's console output to a text file.

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

Shut down the impaired controller

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

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

About this task

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

  [ONTAP 9 NetApp Encryption Power Guide](#)

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
        State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
       Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State    #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online        0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
      Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Replace the controller module hardware - AFF A700 and FAS9000

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

Step 1: Remove the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

①	
Cam handle release button	
②	
Cam handle	

1. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

2. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

①	
Controller module cover locking button	

Step 2: Move the boot media

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

Steps

1. Lift the black air duct at the back of the controller module and then locate the boot media using the following illustration or the FRU map on the controller module:

①	
Press release tab	

②	
Boot media	

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

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

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.

4. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

Step 3: Move the system DIMMs

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

Steps

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

2. Locate the DIMMs on your controller module.

3. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.

4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

❶
DIMM ejector tabs
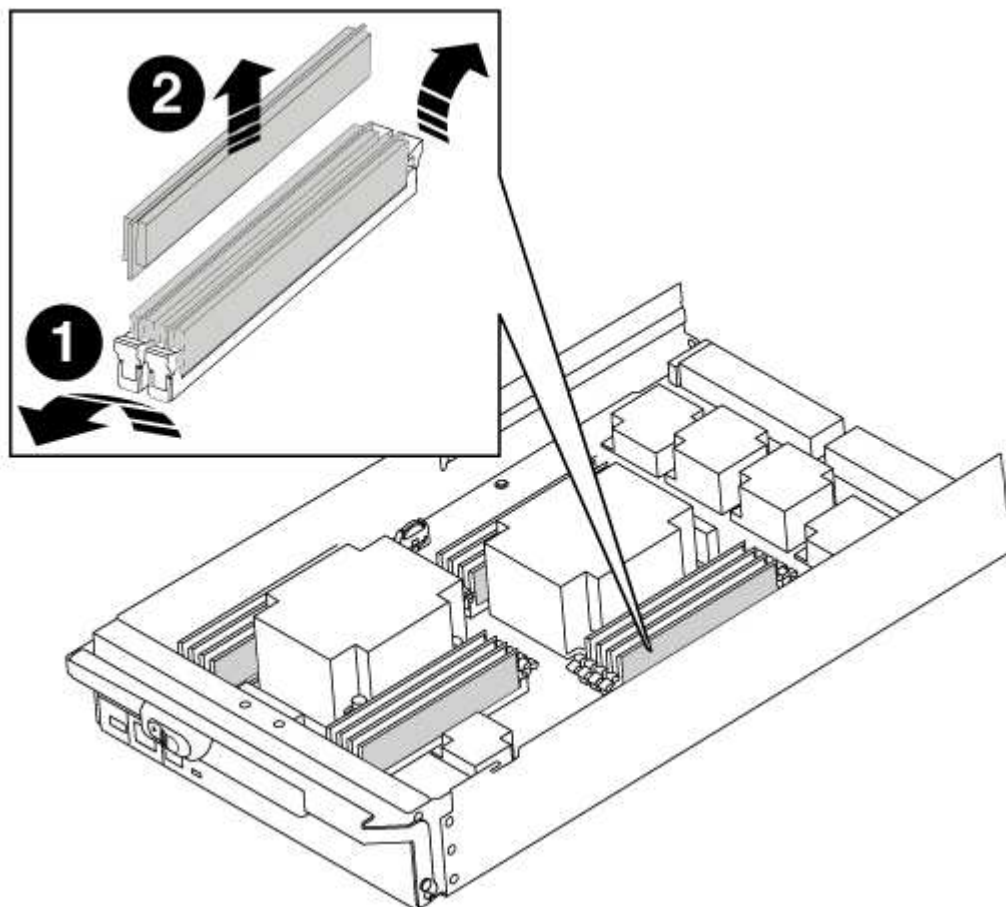
❷
DIMM

5. Locate the slot where you are installing the DIMM.

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

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

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

7. Insert the DIMM squarely into the slot.

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

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

8. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

9. Repeat these steps for the remaining DIMMs.

Step 4: Install the controller

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

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

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

Steps

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

2. If you have not already done so, replace the cover on the controller module.

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

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

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

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

5. Complete the reinstallation of the controller module:

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

   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

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

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

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

Restore and verify the system configuration - AFF A700 and FAS9000

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

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

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

About this task

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

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

Steps

1. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.

2. On the *healthy* node, check the system time: `show date`

   The date and time are given in GMT.

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

   The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date mm/dd/yyyy`

5. If necessary, set the time in GMT on the replacement node: `set time hh:mm:ss`

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

   The date and time are given in GMT.

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

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

Steps

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

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

   - `ha`

   - `mcc`

   - `mcc-2n`

   - `mccip`

   - `non-ha`

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

Step 3: Run system-level diagnostics

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

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

Steps

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

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

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

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

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`

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

   - `bootmedia` is the system booting device.

   - `cna` is a Converged Network Adapter or interface not connected to a network or storage device.

   - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.

- ◦ `env` is motherboard environmentals.

- ◦ `mem` is system memory.

- ◦ `nic` is a network interface card.

- ◦ `nvram` is nonvolatile RAM.

- ◦ `nvmem` is a hybrid of NVRAM and system memory.

- ◦ `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on…	Then…
Individual components	a. Clear the status logs: `sldiag device clearstatus` b. Display the available tests for the selected devices: `sldiag device show -dev _dev_name` `dev_name` can be any one of the ports and devices identified in the preceding step. c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only` `-selection only` disables all other tests that you do not want to run for the device. d. Run the selected tests: `sldiag device run -dev dev_name` After the test is complete, the following message is displayed: <pre>*> <SLDIAG:_ALL_TESTS_COMPLETED></pre> e. Verify that no tests failed: `sldiag device status -dev dev_name -long -state failed` System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

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

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

If the system-level diagnostics tests…	Then…
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br><br>b. Verify that the log was cleared: `sldiag device status`<br><br>　The following default response is displayed:<br><br>```
SLDIAG: No log messages are present.
```<br><br>c. Exit Maintenance mode: `halt`<br><br>　The node displays the LOADER prompt.<br><br>d. Boot the node from the LOADER prompt: `bye`<br><br>e. Return the node to normal operation: |
An HA pair	Perform a give back: `storage failover giveback -ofnode` *replacement_node_name* ⓘ　If you disabled automatic giveback, re-enable it with the `storage failover modify` command.
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

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

Recable the system and reassign disks - AFF A700 and FAS9000

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

Step 1: Recable the system

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

Steps

1. Recable the system.

2. Verify that the cabling is correct by using Active IQ Config Advisor.

   a. Download and install Config Advisor.

   b. Enter the information for the target system, and then click Collect Data.

   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

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

Step 2: Reassign disks

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

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

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

2. From the LOADER prompt on the *replacement* node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.`boot_ontap`

3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

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

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

4. From the healthy node, verify that any coredumps are saved:

   a. Change to the advanced privilege level: `set -privilege advanced`

      You can respond `Y` when prompted to continue into advanced mode. The advanced mode prompt

appears (*>).

b. Save any coredumps: `system node run -node` *local-node-name* `partner savecore`

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

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

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   This is required if both of the following are true:

   ◦ The MetroCluster configuration is in a switchover state.

   ◦ The *replacement* node is the current owner of the disks on the disaster site.

   [Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration](#)

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

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

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

4 entries were displayed.
```

10. Verify that the expected volumes are present for each node: `vol show -node node-name`

11. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Complete system restoration - AFF A700 and FAS9000

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

Step 1: Install licenses for the replacement node in ONTAP

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

About this task

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

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

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

If the node is in a MetroCluster configuration and all nodes at a site have been replaced, license keys must be installed on the *replacement* node or nodes prior to switchback.

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

   NetApp Support

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

Steps

1. Install each license key: `system license add -license-code license-key, license-key...`
2. Remove the old licenses, if desired:

   a. Check for unused licenses: `license clean-up -unused -simulate`

   b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Restoring Storage and Volume Encryption functionality

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

Step

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

   - Restore onboard key management encryption keys
   - Restore external key management encryption keys

Step 3: Verifying LIFs and registering the serial number

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

Steps

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

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

2. Register the system serial number with NetApp Support.

   - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
   - If AutoSupport is not enabled, call NetApp Support to register the serial number.

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

Step 4 (MetroCluster only): Switching back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

   ```
   cluster_B::>  metrocluster node show

   DR                             Configuration  DR
   Group Cluster Node             State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 controller_A_1 configured     enabled   heal roots
   completed
         cluster_B
                 controller_B_1 configured     enabled   waiting for
   switchback recovery
   2 entries were displayed.
   ```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster                     Configuration State     Mode
--------------------        -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster                     Configuration State     Mode
--------------------        -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Return the failed part to NetApp

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.

Hot-swap a de-stage controller power module (DCPM) - AFF A700 and FAS9000

To hot-swap a de-stage controller power module (DCPM), which contains the NVRAM10 battery, you must locate the failed DCPM module, remove it from the chassis, and install the replacement DCPM module.

You must have a replacement DCPM module in-hand before removing the failed module from the chassis and it must be replaced within five minutes of removal. Once the DCPM module is removed from the chassis, there is no shutdown protection for the controller module that owns the DCPM module, other than failover to the other controller module.

Replacing the DCPM module

To replace the DCPM module in your system, you must remove the failed DCPM module from the system and then replace it with a new DCPM module.

Steps

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

2. Remove the bezel on the front of the system and set it aside.

3. Locate the failed DCPM module in the front of the system by looking for the Attention LED on the module.

The LED will be steady amber if the module is faulty.

> ⓘ The DCPM module must be replaced in the chassis within five minutes of removal or the associated controller will shut down.

4. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.

1	DCPM module orange locking button

5. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.

> ⓘ The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

The DCPM module LED lights when the module is fully seated into the chassis.

Dispose of batteries

You must dispose of batteries according to the local regulations regarding battery recycling or disposal. If you cannot properly dispose of batteries, you must return the batteries to NetApp, as described in the RMA instructions that are shipped with the kit.

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Return the failed part to NetApp

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 A700 and FAS9000

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

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

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

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

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

About this task

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
        State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
      Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online        0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
      Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

❶	Cam handle release button

2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

1	Controller module cover locking button

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

Steps

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

2. Locate the DIMMs on your controller module.

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

1 2 3 4

5 6 7 8

9 10 11 12

13 14 15 16

DIMM-1
DIMM-2
DIMM-3
DIMM-4

DIMM-5
DIMM-6
DIMM-7
DIMM-8

DIMM-9
DIMM-10
DIMM-11
DIMM-12

DIMM-13
DIMM-14
DIMM-15
DIMM-16

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.

❶	DIMM ejector tabs
❷	DIMM

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

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

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

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

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

6. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

7. Close the controller module cover.

Step 4: Install the controller

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

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

Steps

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

2. If you have not already done so, replace the cover on the controller module.

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

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

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

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

5. Complete the reinstallation of the controller module:

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

   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

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

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

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

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

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

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

Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

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

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

Steps

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:

a. Select the Maintenance mode option from the displayed menu.

b. After the node boots to Maintenance mode, halt the node: `halt`

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

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

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

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

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

3. Run diagnostics on the system memory: `sldiag device run -dev mem`

4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

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

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

If the system-level diagnostics tests…	Then…
Were completed without any failures	a. Clear the status logs: `sldiag device clearstatus` b. Verify that the log was cleared: `sldiag device status` The following default response is displayed: *SLDIAG: No log messages are present.* a. Exit Maintenance mode: `halt` The node displays the LOADER prompt. b. Boot the node from the LOADER prompt: `bye` c. Return the node to normal operation.
An HA pair	Perform a give back: `storage failover giveback -ofnode` *replacement_node_name* > (i) If you disabled automatic giveback, re-enable it with the storage failover modify command.

If the system-level diagnostics tests…	Then…
A two-node MetroCluster configuration	Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process.
A stand-alone configuration	Proceed to the next step. No action is required. You have completed system-level diagnostics.

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

Step 6: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster                 Configuration State     Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster                    Configuration State     Mode
--------------------        -------------------        ---------
 Local: cluster_B configured              normal
Remote: cluster_A configured              normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 7: Return the failed part to NetApp

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 fan - AFF A700 and FAS9000

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

> (i)   You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

Steps

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

2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.

3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.

4. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

> (!)   The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.

①	Orange release button

5. Set the fan module aside.

6. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

   When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

7. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

8. 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 an I/O module - AFF A700 and FAS9000

To replace an I/O module, you must perform a specific sequence of tasks.

- You can use this procedure with all versions of ONTAP supported by your system

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

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

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

About this task

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
        State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
      Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
-----------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
      Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace I/O modules

To replace an I/O module, locate it within the chassis and follow the specific sequence of steps.

Steps

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

2. Unplug any cabling associated with the target I/O module.

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

3. Remove the target I/O module from the chassis:

   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.
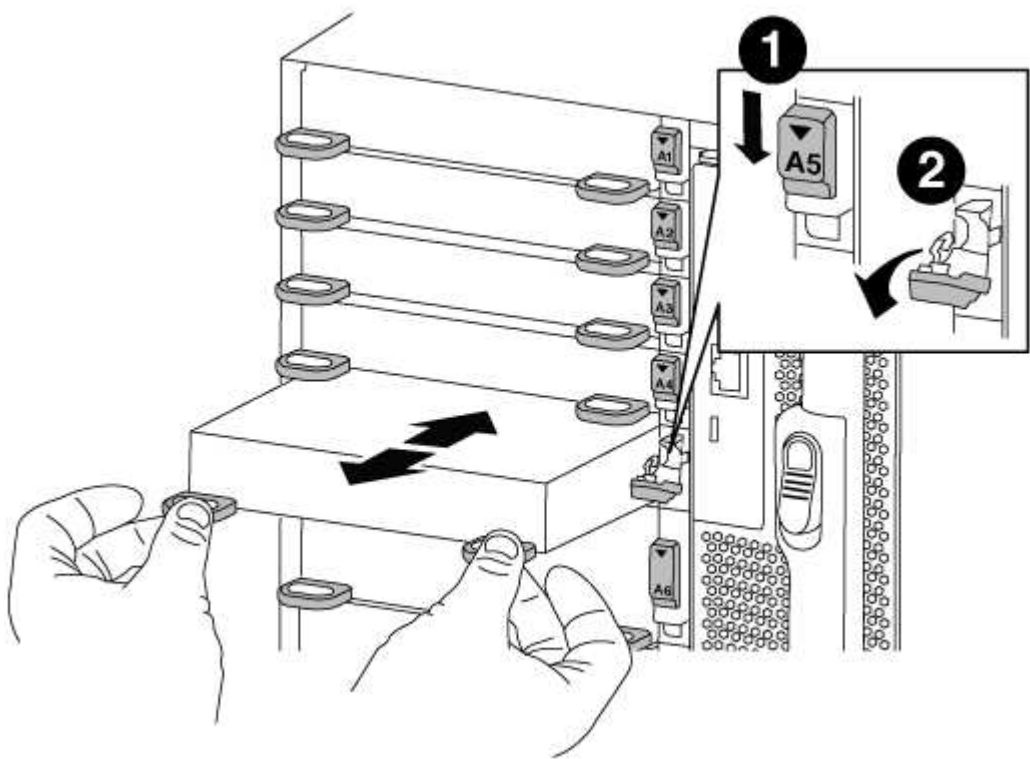
1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

4. Set the I/O module aside.

5. Install the replacement I/O module into the chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

6. Recable the I/O module, as needed.

Step 3: Reboot the controller after PCIe module replacement

After you replace a PCIe module, you must reboot the controller module.

Steps

1. From the LOADER prompt, reboot the node: *bye*

   > ⓘ   This reinitializes the PCIe cards and other components and reboots the node.

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

   > ⓘ   Be sure to exit Maintenance mode after completing the conversion.

3. Return the node to normal operation: `storage failover giveback -ofnode` *impaired_node_name*

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

   > ⓘ   If your system is in a two-node MetroCluster configuration, you must switch back the aggregates as described in the next step.

Step 4: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- --------------  --------------  ---------
-------------------
1     cluster_A
            controller_A_1 configured      enabled    heal roots
completed
      cluster_B
            controller_B_1 configured      enabled    waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster                 Configuration State    Mode
--------------------    -------------------    ---------
 Local: cluster_B configured       switchover
Remote: cluster_A configured       waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster                 Configuration State    Mode
--------------------    -------------------    ---------
 Local: cluster_B configured          normal
Remote: cluster_A configured          normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

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 an LED USB module - AFF A700 and FAS9000

You can replace an LED USB module without interrupting service.

The FAS9000 or AFF A700 LED USB module provides connectivity to console ports and system status. Replacement of this module does not require tools.

Steps

1. Remove the old LED USB module:

   a. With the bezel removed, locate the LED USB module at the front of the chassis, on the bottom left side.

   b. Slide the latch to partially eject the module.

   c. Pull the module out of the bay to disconnect it from the midplane. Do not leave the slot empty.

2. Install the new LED USB module:

   a. Align the module to the bay with the notch in the corner of the module positioned near the slider latch on the chassis. The bay will prevent you from installing the module upside down.

b. Push the module into the bay until it is fully seated flush with the chassis.

There is an audible click when the module is secure and connected to the midplane.

Return the failed part to NetApp

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 or NVRAM DIMMs - AFF A700 and FAS9000

The NVRAM module consists of the NVRAM10 and DIMMs and up to two NVMe SSD Flash Cache modules (FlashCache or caching modules) per NVRAM module. You can replace a failed NVRAM module or the DIMMs inside the NVRAM module. To replace a failed NVRAM module, you must remove it from the chassis, remove the FlashCache module or modules from the NVRAM module, move the DIMMs to the replacement module, reinstall the FlashCache module or modules, and install the replacement NVRAM module into the chassis. Because the system ID is derived from the NVRAM module, if replacing the module, disks belonging to the system are reassigned to the new system ID.

Before you begin

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

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using one of the following options.

Option 1: Most systems

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

About this task

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a Two-node MetroCluster

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
        State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
      Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online        0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
      Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace the NVRAM module

To replace the NVRAM module, locate it in slot 6 in the chassis and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Move the FlashCache module from the old NVRAM module to the new NVRAM module:
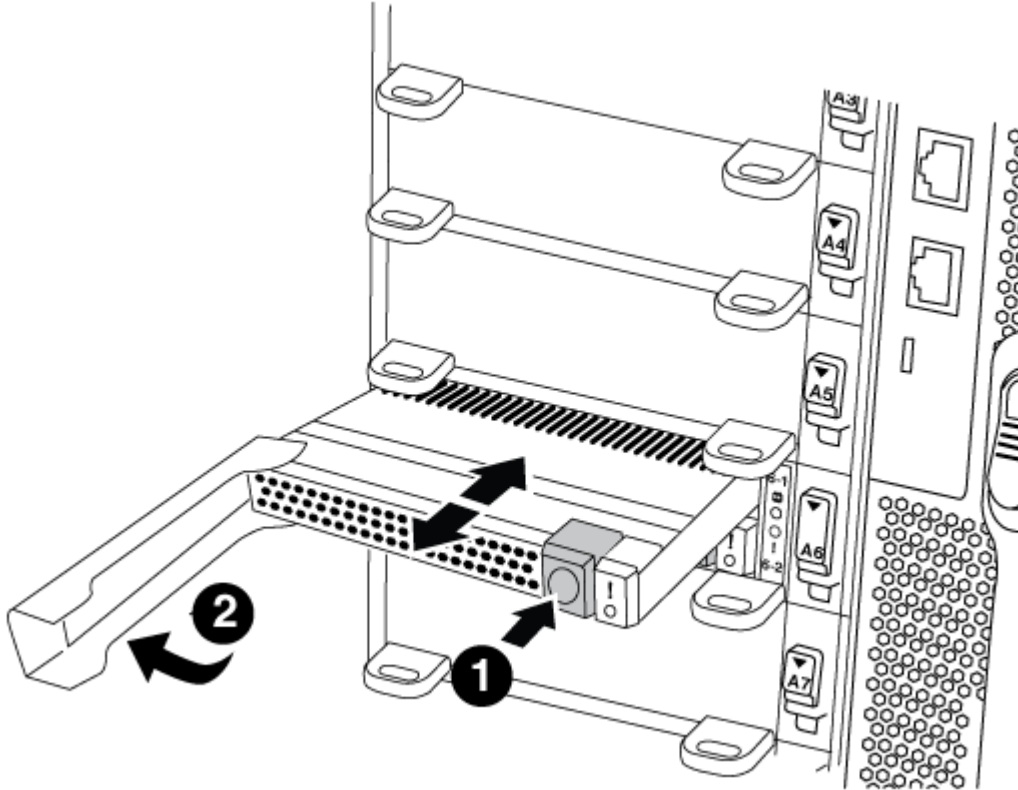
1	Orange release button (gray on empty FlashCache modules)
2	FlashCache cam handle

    a. Press the orange button on the front of the FlashCache module.

> ⓘ The release button on empty FlashCache modules is gray.

    b. Swing the cam handle out until the module begins to slide out of the old NVRAM module.

    c. Grasp the module cam handle and slide it out of the NVRAM module and insert it into the front of the new NVRAM module.

    d. Gently push the FlashCache module all the way into the NVRAM module, and then swing the cam

handle closed until it locks the module in place.

3. Remove the target NVRAM module from the chassis:

   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The NVRAM module disengages from the chassis and moves out a few inches.

   c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

❶	Lettered and numbered I/O cam latch
❷	I/O latch completely unlocked

4. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.

1	Cover locking button
2	DIMM and DIMM ejector tabs

5. Remove the DIMMs, one at a time, from the old NVRAM module and install them in the replacement NVRAM module.

6. Close the cover on the module.

7. Install the replacement NVRAM module into the chassis:

   a. Align the module with the edges of the chassis opening in slot 6.

   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

Step 3: Replace a NVRAM DIMM

To replace NVRAM DIMMs in the NVRAM module, you must remove the NVRAM module, open the module, and then replace the target DIMM.

Steps

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

2. Remove the target NVRAM module from the chassis:

   a. Depress the lettered and numbered cam button.

   The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

   The NVRAM module disengages from the chassis and moves out a few inches.

c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

❶	Lettered and numbered I/O cam latch
❷	I/O latch completely unlocked

3. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.

❶	Cover locking button
❷	DIMM and DIMM ejector tabs

4. Locate the DIMM to be replaced inside the NVRAM module, and then remove it by pressing down on the DIMM locking tabs and lifting the DIMM out of the socket.

   Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.

6. Close the cover on the module.

7. Install the replacement NVRAM module into the chassis:

   a. Align the module with the edges of the chassis opening in slot 6.

   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

Step 4: Reboot the controller after FRU replacement

After you replace the FRU, you must reboot the controller module.

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Reassign disks

Depending on whether you have an HA pair or two-node MetroCluster configuration, you must either verify the reassignment of disks to the new controller module or manually

reassign the disks.

Select one of the following options for instructions on how to reassign disks to the new controller.

Option 1: Verify ID (HA pair)

Verify the system ID change on an HA system

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

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

Steps

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

2. From the LOADER prompt on the replacement node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.

   `boot_ontap bye`

   The node will reboot, if autoboot is set.

3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned: `storage failover show`

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

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

4. From the healthy node, verify that any coredumps are saved:

   a. Change to the advanced privilege level: `set -privilege advanced`

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

   b. Save any coredumps: `system node run -node` *local-node-name* `partner savecore`

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

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

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

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the node:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   This is required if both of the following are true:

   ◦ The MetroCluster configuration is in a switchover state.

   ◦ The *replacement* node is the current owner of the disks on the disaster site.

     [Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration](#)

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

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

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

   4 entries were displayed.
   ```

10. Verify that the expected volumes are present for each node: `vol show -node node-name`

11. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Option 2: Reassign ID (MetroCluster config)

Reassign the system ID in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

• The *impaired* node is the node on which you are performing maintenance.

• The *replacement* node is the new node that replaced the impaired node as part of this procedure.

• The *healthy* node is the DR partner of the impaired node.

Steps

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by entering

`Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.

You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node: `metrocluster node show -fields node-systemid,dr-partner-systemid`

In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

```
dr-group-id cluster          node                    node-systemid dr-
partner-systemid
 ----------- -------------------- --------------------
------------- --------------------
 1          Cluster_A            Node_A_1                536872914
118073209
 1          Cluster_B            Node_B_1                118073209
536872914
 2 entries were displayed.
```

3. View the new system ID at the Maintenance mode prompt on the impaired node: `disk show`

In this example, the new system ID is 118065481:

```
Local System ID: 118065481
    ...
    ...
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

In the case of the preceding example, the command is: `disk reassign -s 118073209`

You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

Verify that the disks belonging to the *replacement* node show the new system ID for the *replacement* node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

```
*> disk show -a
Local System ID: 118065481

  DISK        OWNER                      POOL     SERIAL NUMBER   HOME
-------      -------------              -----    -------------   -------------
disk_name   system-1  (118065481) Pool0   J8Y0TDZC         system-1
(118065481)
disk_name   system-1  (118065481) Pool0   J8Y09DXC         system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:

   a. Change to the advanced privilege level: `set -privilege advanced`

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

   b. Verify that the coredumps are saved: `system node run -node` *local-node-name* `partner savecore`

      If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node` *local-node-name* `partner savecore -s command.</info>`.

   c. Return to the admin privilege level: `set -privilege admin`

7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`

8. Boot the *replacement* node: `boot_ontap`

9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`

10. Verify the MetroCluster configuration: `metrocluster node show - fields configuration-state`

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

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

4 entries were displayed.
```

11. Verify the operation of the MetroCluster configuration in Data ONTAP:

    a. Check for any health alerts on both clusters: `system health alert show`

    b. Confirm that the MetroCluster is configured and in normal mode: `metrocluster show`

    c. Perform a MetroCluster check: `metrocluster check run`

    d. Display the results of the MetroCluster check: `metrocluster check show`

    e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

       After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Simulate a switchover operation:

    a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`

       You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

    b. Perform the switchback operation with the -simulate parameter: `metrocluster switchover -simulate`

    c. Return to the admin privilege level: `set -privilege admin`

Step 6: Restore Storage and Volume Encryption functionality

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

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.

2. Use one of the following procedures, depending on whether you are using onboard or external key

management:

- ◦ Restore onboard key management encryption keys
- ◦ Restore external key management encryption keys

Step 7: Return the failed part to NetApp

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 A700 and FAS9000

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

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

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

> (i) 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.

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

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:

   a. Turn off the power switch on the power supply.

   b. Open the power cable retainer, and then unplug the power cable from the power supply.

   c. Unplug the power cable from the power source.

4. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.

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

	Locking button

5. Make sure that the on/off switch of the new power supply is in the Off position.

6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

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

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

7. Reconnect the power supply cabling:

   a. Reconnect the power cable to the power supply and the power source.

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

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

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

   The green power LED lights when the PSU is fully inserted into the chassis and the amber attention LED flashes initially, but turns off after a few moments.

9. 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

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

- You can use this procedure with all versions of ONTAP supported by your system

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

Step 1: Shut down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Option 1: Most configurations

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

About this task

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

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

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

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

Steps

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.

- You must leave the power supplies turned on at the end of this procedure to provide power to the healthy controller.

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller…	Then…
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: `metrocluster switchover`
Has not automatically switched over, you attempted switchover with the `metrocluster switchover` command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
        State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
      Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the -override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
       State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
      Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

1	Cam handle release button

2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.

1	Controller module cover locking button

Step 3: Replace the RTC battery

To replace the RTC battery, you must locate the failed battery in the controller module, remove it from the holder, and then install the replacement battery in the holder.

Steps

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

1	RTC battery
2	RTC battery housing

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

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

4. Remove the replacement battery from the antistatic shipping bag.

5. Locate the empty battery holder in the controller module.

6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.

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

8. Reinstall the controller module cover.

Step 4: Reinstall the controller module and set time/date

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

Steps

1. If you have not already done so, close the air duct or controller module cover.

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

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

3. Recable the system, as needed.

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

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.

5. Complete the reinstallation of the controller module:

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

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

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

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

   d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.

   e. Halt the controller at the LOADER prompt.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy node with the `show date` command.

   b. At the LOADER prompt on the target node, check the time and date.

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

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

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

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the node reboot.

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

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

Step 5: Switch back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled` state: `metrocluster node show`

```
cluster_B::>  metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- --------------     --------------  ---------
--------------------
1     cluster_A
            controller_A_1 configured     enabled   heal roots
completed
      cluster_B
            controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`

4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

5. Verify that the switchback operation has completed: `metrocluster show`

   The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster                  Configuration State     Mode
--------------------     -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster                  Configuration State     Mode
--------------------     -------------------     ---------
 Local: cluster_B configured              normal
Remote: cluster_A configured              normal
```

   If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

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.

X91148A module

Overview of adding an X91148A module - AFF A9000

You can add an I/O module to your system by either replacing a NIC or storage adapter with a new one in a fully-populated system, or by adding a new NIC or storage adapter into an empty chassis slot in your system.

Before you begin

- Check the NetApp Hardware Universe to make sure that the new I/O module is compatible with your system and version of ONTAP you're running.

- If multiple slots are available, check the slot priorities in NetApp Hardware Universe and use the best one available for your I/O module.

- To non-disruptively add an I/O module, you must takeover the target controller, remove the slot blanking cover in the target slot or remove an existing I/O module, add the new or replacement I/O module, and then giveback the target controller.

- Make sure that all other components are functioning properly.

Add an X91148A module in an AFF A700 with open slots - AFF A700 and FAS9000

You can add an X91148A module into an empty module slot in your system as either a 100GbE NIC or a storage module for the NS224 storage shelves.

- Your system must be running ONTAP 9.8 and later.

- To non-disruptively add the X91148A module, you must takeover the target controller, remove the slot blanking cover in the target slot, add the module, and then giveback the target controller.

- There must be one or more open slots available on your system.

- If multiple slots are available, install the module according to the slot priority matrix for the X91148A module in the Hardware Universe.

  NetApp Hardware Universe

- If you are adding the X91148A module as a storage module, you must install the module slots 3 and/or 7.

- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node` *node name* `-port` *port name* `-mode network` command. See the Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

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

Option 1: Add an X91148A module as a NIC module in a system with open slots

To add an X91148A module as a NIC module in a system with open slots, you must follow the specific sequence of steps.

Steps

1. Shutdown controller A:

   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

3. Remove the target slot blanking cover:

   a. Depress the lettered and numbered cam button.

   b. Rotate the cam latch down until it is in a horizontal position.

   c. Remove the blanking cover.

4. Install the X91148A module:

   a. Align the X91148A module with the edges of the slot.

   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.

   c. Push the I/O cam latch all the way up to lock the module in place.

5. Cable the module to the data switches.

6. Reboot controller A: `boot_ontap`

7. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`

8. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto-giveback true`

9. Repeat these steps for controller B.

Option 2: Add an X91148A module as a storage module in a system with open slots

To add an X91148A module as a storage module in a system with open slots, you must follow the specific sequence of steps.

- This procedure presumes slots 3 and/or 7 are open.

Steps

1. Shut down controller A:

   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

3. Remove the target slot blanking cover:

    a. Depress the lettered and numbered cam button.

    b. Rotate the cam latch down until it is in a horizontal position.

    c. Remove the blanking cover.

4. Install the X91148A module into slot 3:

    a. Align the X91148A module with the edges of the slot.

    b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.

    c. Push the I/O cam latch all the way up to lock the module in place.

    d. If you are installing a second X91148A module for storage, repeat this step for the module in slot 7.

5. Reboot controller A: `boot_ontap`

6. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`

7. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`

8. Repeat these steps for controller B.

9. Install and cable your NS224 shelves, as described in Hot-add - NS224 shelves.

Add an X91148A storage module in a system with no open slots - AFF A700 and FAS9000

You must remove one more or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- Your system must be running ONTAP 9.8 and later.

- To non-disruptively add the X91148A module, you must takeover the target controller, add the module, and then giveback the target controller.

- If you are adding the X91148A module as a storage adapter, you must install the module in slots 3 and/or 7.

- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node` *node name* `-port` *port name* `-mode network` command for each port. See the Hardware Universe for other slots that can be used by the X91148A module for networking.

    NetApp Hardware Universe

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

Option 1: Add an X91148A module as a NIC module in a system with no open slots

You must remove one or more existing NIC or storage modules in your system in order to install one or more X91148A NIC modules into your fully-populated system.

Steps

1. If you are adding an X91148A module into a slot that contains a NIC module with the same number of ports as the X91148A module, the LIFs will automatically migrate when its controller module is shut down. If the NIC module being replaced has more ports than the X91148A module, you must permanently reassign the affected LIFs to a different home port. See Migrating a LIF for information about using System Manager to permanently move the LIFs

2. Shut down controller A:

   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

   b. Take over the target node: `storage failover takeover -ofnode` *target_node_name*

      The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

4. Unplug any cabling on the target I/O module.

5. Remove the target I/O module from the chassis:

   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

      Make sure that you keep track of which slot the I/O module was in.

❶	Lettered and numbered I/O cam latch
❷	I/O cam latch completely unlocked

6. Install the X91148A module into the target slot:

   a. Align the X91148A module with the edges of the slot.

   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.

   c. Push the I/O cam latch all the way up to lock the module in place.

7. Repeat the remove and install steps to replace additional modules for controller A.

8. Cable the module or modules to the data switches.

9. Reboot controller A: `boot_ontap`

10. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`

11. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`

12. If you added the X91148A module as a NIC module in slots 3 or 7, for networking, use the `storage port modify -node` *node name* `-port` *port name* `-mode network` command for each port.

13. Repeat these steps for controller B.

Option 2: Adding an X91148A module as a storage module in a system with no open slots

You must remove one or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- This procedure presumes you re installing the X91148A module into slots 3 and/or 7.

Steps

1. If you are adding an X91148A module as a storage module in slots 3 and/or 7 into a slot that has an existing NIC module in it, use System Manager to permanently migrate the LIFs to different home ports, as described in Migrating a LIF.

2. Shut down controller A:

   a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

   b. Take over the target node: `storage failover takeover -ofnode target_node_name`

   The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

4. Unplug any cabling on the target I/O module.

5. Remove the target I/O module from the chassis:

   a. Depress the lettered and numbered cam button.

   The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

   The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

   Make sure that you keep track of which slot the I/O module was in.

1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

6. Install the X91148A module into slot 3:

   a. Align the X91148A module with the edges of the slot.

   b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.

   c. Push the I/O cam latch all the way up to lock the module in place.

   d. If you are installing a second X91148A module for storage, repeat the remove and install steps for the module in slot 7.

7. Reboot controller A: `boot_ontap`

8. Giveback the node from the partner node: `storage failover giveback -ofnode` *target_node_name*

9. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`

10. Repeat these steps for controller B.

11. Install and cable your NS224 shelves, as described in Hot-adding an NS224 drive shelf.