



Boot media

ONTAP Systems

NetApp
February 22, 2022

Table of Contents

- Boot media 1
 - Overview of boot media replacement - AFF A400 1
 - Check onboard encryption - AFF A400 1
 - Shut down the impaired controller - AFF A400..... 5
 - Replace the boot media - AFF A400 8
 - Boot the recovery image - AFF A400 13
 - Switch back aggregates in a two-node MetroCluster configuration - AFF A400 16
 - Restore OKM, NSE, and NVE as needed - AFF A400..... 17
 - Return the failed part to NetApp - AFF A400 21

Boot media

Overview of boot media replacement - AFF A400

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` file.

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 must be connected to a network to restore the `var` file system.
 - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct 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 - AFF A400

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

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

Steps

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

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

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

3. Check the version of ONTAP the system is running on the impaired node if up, or on the partner node if the impaired node is down, using the `version -v` command:
 - If `<No-DARE>` or `<1Ono-DARE>` is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
 - If `<No-DARE>` is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.
4. If the impaired node is part of an HA configuration, disable automatic giveback from the healthy node:
`storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

Check NVE or NSE on systems running ONTAP 9.6 and later

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

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

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

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

Verify NVE configuration

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



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

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

you need to complete some additional steps.

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

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

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

If the command fails, contact NetApp Support.

mysupport.netapp.com

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

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

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



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

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

Verify NSE configuration

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



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

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

If the command fails, contact NetApp Support.

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

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

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

Shut down the impaired controller - AFF A400

Option 1: Most configurations

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

Steps

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

If the impaired node displays...	Then...
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt (enter system password)	<p>Take over or halt the impaired node from the healthy node: <code>storage failover takeover -ofnode impaired_node_name</code></p> <p>+ When the impaired node shows Waiting for giveback..., press Ctrl-C, and then respond <code>y</code>.</p> <p>+</p>

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



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

Option 2: Controller is in a MetroCluster configuration

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



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

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

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

Steps

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

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

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:>`

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

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

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

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.

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

Steps

1. Check the MetroCluster status to determine whether the impaired node has automatically switched over to the healthy node: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired node...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy node: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> 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 boot media - AFF A400

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

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

[Removing the controller module](#)

Steps

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

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

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

The controller module moves slightly out of the chassis.



1	Locking latches
2	Slide controller out of chassis

- 6. Slide the controller module out of the chassis.

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

- 7. Place the controller module on a stable, flat surface.

Step 2: Replace the boot media

You must locate the boot media in the controller module (see the FRU map on the

controller module), and then follow the directions to replace it.

Before you begin

Although the contents of the boot media is encrypted, it is a best practice to erase the contents of the boot media before replacing it. For more information, see the [Statement of Volatility](#) for your system on the NetApp Support Site.



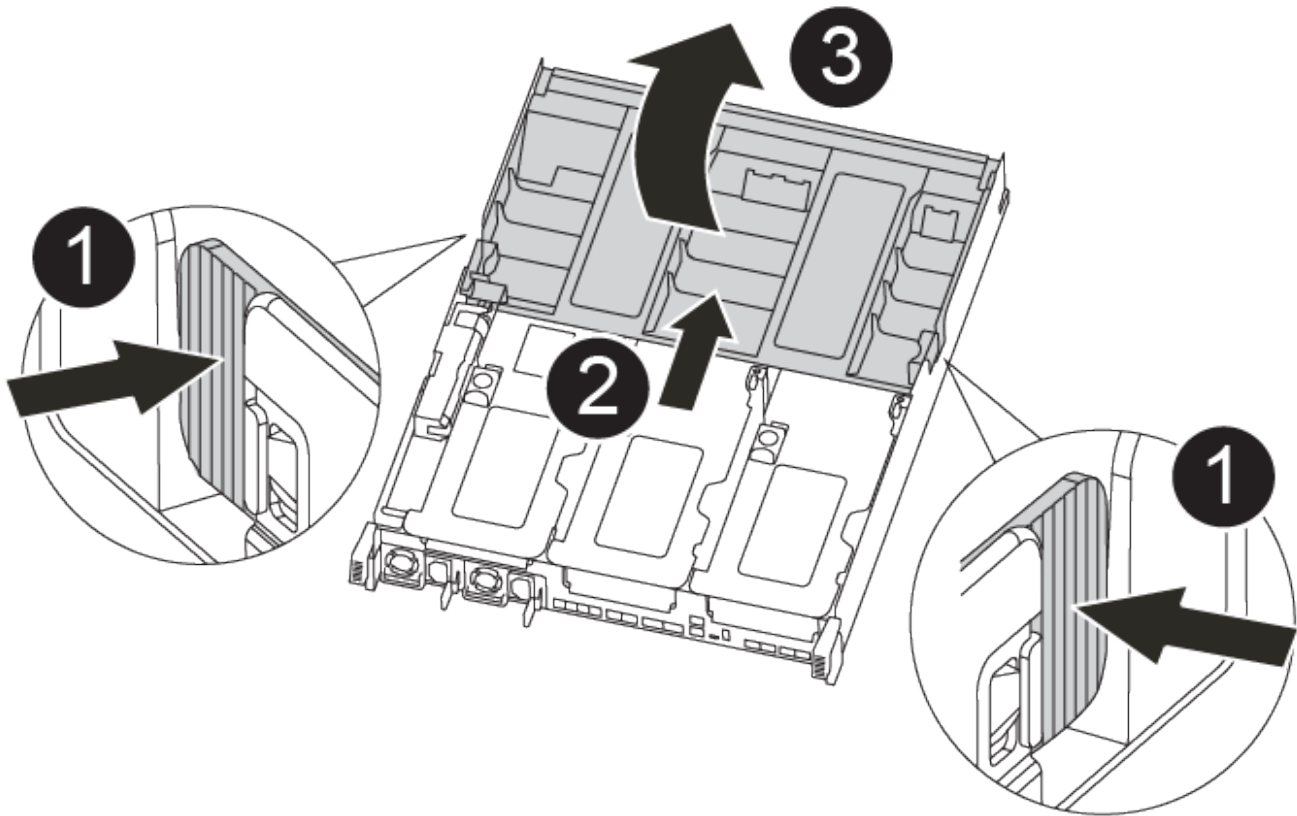
You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the boot media.

[Replacing the boot media](#)

Steps

1. Open the air duct:



1	Locking tabs
2	Slide air duct toward back of controller
3	Rotate air duct up

- a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
- b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely

open position.

2. Locate and remove the boot media from the controller module:



1	Press blue button
2	Rotate boot media up and remove from socket

- Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
 - Rotate the boot media up and gently pull the boot media out of the socket.
- Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
 - Check the boot media to make sure that it is seated squarely and completely in the socket.

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

5. Lock the boot media in place:

- Rotate the boot media down toward the motherboard.
- Placing a finger at the end of the boot media by the blue button, push down on the boot media end to engage the blue locking button.
- While pushing down on the boot media, lift the blue locking button to lock the boot media in place.

6. Close the air duct.

Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed does not have a boot image, so you need to transfer a boot image using a USB flash drive.

Before you begin

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

Steps

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



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

There are two folders in the unzipped service image file:

- `boot`
- `efi`

- c. Copy the `efi` folder to the top directory on the USB flash drive.

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

- d. Remove the USB flash drive from your laptop.
2. If you have not already done so, close the air duct.
 3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
 4. Reinstall the cable management device and recable the system, as needed.

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

5. Plug the power cable into the power supply and reinstall the power cable retainer.
6. Insert the USB flash drive into the USB slot on the controller module.

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

7. Complete the installation of the controller module:

- a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
- 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. If you have not already done so, reinstall the cable management device.

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

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

9. 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 A400

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: 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	<ol style="list-style-type: none"> a. Press <code>y</code> when prompted to restore the backup configuration. b. Set the healthy node to advanced privilege level: <code>set -privilege advanced</code> c. Run the restore backup command: <code>system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code> d. Return the node to admin level: <code>set -privilege admin</code> e. Press <code>y</code> when prompted to use the restored configuration. f. Press <code>y</code> when prompted to reboot the node.
No network connection	<ol style="list-style-type: none"> a. Press <code>n</code> 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. <p>If you are prompted to continue with the update, press <code>y</code>.</p>

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.

If you see...	Then...
Waiting for giveback...	<ol style="list-style-type: none"> Log into the partner node. Confirm the target node is ready for giveback with the <code>storage failover show</code> command.

- Connect the console cable to the partner node.
- Give back the node using the `storage failover giveback -fromnode local` command.
- 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.

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

Option 2: Controller is in a two-node MetroCluster

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

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

The image is downloaded from the USB flash drive.

- When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
- After the image is installed, start the restoration process:
 - Press `n` when prompted to restore the backup configuration.
 - Press `y` when prompted to reboot to start using the newly installed software.

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

- 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.
- Verify that the environmental variables are set as expected.
 - Take the node to the LOADER prompt.
 - Check the environment variable settings with the `printenv` command.
 - 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 A400

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 Group	Cluster	Node	Configuration State	DR Mirroring Mode
1	cluster_A	controller_A_1	configured	enabled
completed				
	cluster_B	controller_B_1	configured	enabled
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 A400

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 [Restore NVE or NSE when Onboard Key Manager is enabled](#).
 - If NSE or NVE are enabled for ONTAP 9.6, go to [Restore NSE/NVE on systems running ONTAP 9.6 and later](#).

Restore NVE or NSE when Onboard Key Manager is enabled

Steps

- Connect the console cable to the target node.
- Use the `boot_ontap` command at the LOADER prompt to boot the node.
- Check the console output:

If the console displays...	Then...
The LOADER prompt	Boot the node to the boot menu: <code>boot_ontap menu</code>

If the console displays...	Then...
Waiting for giveback....	<ol style="list-style-type: none"> Enter <code>Ctrl-C</code> at the prompt At the message: Do you wish to halt this node rather than wait [y/n]? , enter: <code>y</code> At the LOADER prompt, enter the <code>boot_ontap</code> menu command.

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



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

Example of backup data:

```
-----BEGIN BACKUP-----
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOIH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TIYFss4PDjTaV
dzRYkLd1PhQLxAWJwOlyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAGAZJEIwvdeHr5RCavHGclo+wAAAAAAAAA
lgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAAGAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAA
-----END BACKUP-----
```

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

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

- Move the console cable to the partner node and login as "admin".
- Confirm the target node is ready for giveback with the `storage failover show` command.
- Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
 - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.

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



Terminating CIFS can cause loss of data.

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

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

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

12. Move the console cable to the target node.

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



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

- d. Wait 10 minutes for the key to synchronize across the cluster.

13. Move the console cable to the partner node.

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

15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

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

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

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

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

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

Restore NSE/NVE on systems running ONTAP 9.6 and later

Steps

1. Connect the console cable to the target node.
2. Use the `boot_ontap` command at the LOADER prompt to boot the node.

3. Check the console output:

If the console displays...	Then...
The login prompt	Go to Step 7.
Waiting for giveback...	<ul style="list-style-type: none">a. Log into the partner node.b. Confirm the target node is ready for giveback with the <code>storage failover show</code> command.

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



Terminating CIFS can cause loss of data.

- If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
 - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home node and port.
- If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.
7. Move the console cable to the target node and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.

- If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
- If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.



If the command fails, contact Customer Support.

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

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

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

Return the failed part to NetApp - AFF A400

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at [NetApp Support](#), 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

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