NetApp

Boot media

Install and maintain

NetApp
August 24, 2022

Table of Contents

Boot media

Overview of boot media replacement - AFF A700s

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

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

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

Check onboard encryption keys - AFF A700s

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

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

Steps

1. Check the status of the impaired controller:
    - If the impaired controller is at the login prompt, log in as `admin`.
    - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
    - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.

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

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

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

- If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.

- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to [Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier].

- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later].

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

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

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

Steps

1. Connect the console cable to the impaired controller.

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

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

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

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

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

Verify NVE configuration

Steps

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

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

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

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

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

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

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

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

c. Shut down the impaired controller.

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

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

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

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

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

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

      ▪ Shut down the impaired controller.

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

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

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

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

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

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

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

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

      ▪ You can safely shutdown the controller.

Verify NSE configuration

Steps

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

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

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

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

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

```
unavailable:
```

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

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

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

c. Shut down the impaired controller.

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

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

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

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

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

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

      ▪ Shut down the impaired controller.

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

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

         (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`

   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.

  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 controller - AFF A700s

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

Steps

a. Take the impaired controller to the LOADER prompt:

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

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

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

Replace the boot media - AFF A700s

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

Step 1: Remove the controller module

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

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

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

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

3. Unplug the controller module power supply from the source, and then unplug the cable from the power supply.

4. Remove the cable management device from the controller module and set it aside.

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

   The controller module moves slightly out of the chassis.

1	Locking latch
2	Locking pin

1. Slide the controller module out of the chassis.

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

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

		Air duct locking tabs
		Risers
		Air duct

Step 2: Replace the boot media - AFF A700s

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

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

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media:

   a. Open the air duct, if needed.

   b. If needed, remove Riser 2, the middle PCIe module, by unlocking the locking latch and then removing the riser from the controller module.

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

3. Locate the failed boot media by the lit LED on the controller module motherboard.

4. Remove the boot media from the controller module:

   a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.

   b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.

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

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

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

7. Rotate the boot media down until it is flush with the motherboard.

8. Secure the boot media in place by using the screw.

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

9. Reinstall the riser into the controller module.

10. Close the air duct:

    a. Rotate the air duct downward.

    b. Slide the air duct toward the risers until it clicks into place.

Transfer the boot image to the boot media - AFF A700s

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

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

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

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

Steps

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

2. If you have not already done so, close the air duct:

    a. Swing the air duct all the way down to the controller module.

    b. Slide the air duct toward the risers until the locking tabs click into place.

    c. Inspect the air duct to make sure that it is properly seated and locked into place.

| ❶ | Air duct |
| ❷ | Risers |

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

4. Reinstall the cable management device and recable the system, as needed.

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

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

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

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

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

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

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

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

   The image is downloaded from the secondary boot media.

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

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

    a. Record the IP address of the impaired controller that is displayed on the screen.

    b. Press `y` when prompted to restore the backup configuration.

    c. Press `y` when prompted to confirm that the backup procedure was successful.

11. From the partner controller in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address impaired_node_IP_address`

12. After the configuration synchronization is complete without errors, press `y` when prompted to confirm that the backup procedure was successful.

13. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.

14. Exit advanced privilege level on the healthy controller.

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

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

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

Steps

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

2. If you have not already done so, close the air duct:

    a. Swing the air duct all the way down to the controller module.

    b. Slide the air duct toward the risers until the locking tabs click into place.

    c. Inspect the air duct to make sure that it is properly seated and locked into place.

❶	Air duct
❷	Risers

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

4. Reinstall the cable management device and recable the system, as needed.

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

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

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

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

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

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

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

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

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

9. Although the environment variables and bootargs are retained, you should check that all required boot environment variables and bootargs are properly set for your system type and configuration using the `printenv bootarg name` command and correct any errors using the `setenv variable-name <value>` command.

   a. Check the boot environment variables:

      - `bootarg.init.boot_clustered`

      - `partner-sysid`

      - `bootarg.init.flash_optimized` for AFF C190/AFF A220 (All Flash FAS)

      - `bootarg.init.san_optimized` for AFF A220 and All SAN Array

      - `bootarg.init.switchless_cluster.enable`

   b. If External Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:

      - `bootarg.storageencryption.support <value>`

      - `bootarg.keymanager.support <value>`

      - `kmip.init.interface <value>`

      - `kmip.init.ipaddr <value>`

      - `kmip.init.netmask <value>`

      - `kmip.init.gateway <value>`

   c. If Onboard Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:

      - `bootarg.storageencryption.support <value>`

      - `bootarg.keymanager.support <value>`

      - `bootarg.onboard_keymanager <value>`

   d. Save the environment variables you changed with the `savenv` command

   e. Confirm your changes using the `printenv variable-name` command.

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

    The image is downloaded from the USB flash drive.

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

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

    a. Record the IP address of the impaired controller that is displayed on the screen.

    b. Press `y` when prompted to restore the backup configuration.

    c. Press `y` when prompted to confirm that the backup procedure was successful.

13. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.

14. From the partner controller in advanced privilege level, start the configuration synchronization using the IP address recorded in the previous step: `system node restore-backup -node local -target -address impaired_node_IP_address`

15. After the configuration synchronization is complete without errors, press `y` when prompted to confirm that the backup procedure was successful.

16. Press `y` when prompted whether to use the restored copy, and then press `y` when prompted to reboot the controller.

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

    a. Take the controller to the LOADER prompt.

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

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

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

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

    e. Reboot the controller.

18. With the rebooted impaired controller displaying the `Waiting for giveback…` message, perform a giveback from the healthy controller:

If your system is in…	Then…

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

19. Exit advanced privilege level on the healthy controller.

Boot the recovery image - AFF A700s

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

the environmental variables.

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

   The image is downloaded from the USB flash drive.

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

3. Restore the var file system:

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

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

   a. Take the controller to the LOADER prompt.

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

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

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

5. The next depends on your system configuration:

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

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

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

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

7. Connect the console cable to the partner controller.

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

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

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

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

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

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

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

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

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

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

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

Steps

1. Connect the console cable to the target controller.

2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.

3. Check the console output:

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

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

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

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

> ℹ️ 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
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1lWgE5DLRqkiAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAIAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
lgAAAAAAAoAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

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

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

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

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.

10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.

- If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.

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

  > (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.

   > (i) 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.

   > (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.

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.

    > (i)   If the command fails, contact Customer Support.

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

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

11. Connect the console cable to the partner controller.

12. Give back the controller using the `storage failover giveback -fromnode local` command.

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

Return the failed part to NetApp - AFF A700s

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