



# **Boot media**

## **ONTAP Systems**

NetApp  
February 17, 2022

# Table of Contents

- Boot media ..... 1
  - Replace the boot media - AFF A320 ..... 1
  - Check onboard encryption keys as needed - AFF A320 ..... 1
  - Shut down the node - AFF A320 ..... 5
  - Remove the controller module, replace the boot media and transfer the boot image to the boot media - AFF A320 ..... 6
  - Boot the recovery image - AFF A320 ..... 12
  - Restore OKM, NSE, and NVE as needed - AFF A320 ..... 14
  - Return the failed part to NetApp - AFF A320 ..... 18

# Boot media

## Replace the boot media - AFF A320

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 keys as needed - AFF A320

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](https://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 go to the next section.

## 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](https://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](https://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](https://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.  
  
[mysupport.netapp.com](https://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.

## Shut down the node - AFF A320

### Option 1: Most systems

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 <code>Ctrl-C</code> , 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 <code>Waiting for giveback...</code>, press <code>Ctrl-C</code>, 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: System is in a MetroCluster

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)	<p>Take over or halt the impaired node from the healthy node: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code></p> <p>+ When the impaired node shows Waiting for giveback..., press Ctrl-C, and then respond <code>y</code>.</p> <p>+</p>

# Remove the controller module, replace the boot media and transfer the boot image to the boot media - AFF A320

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.

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supply from the power source.
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 and set aside the cable management devices from the left and right sides of the controller module.
5. Remove the controller module from the chassis:



- a. Insert your forefinger into the latching mechanism on either side of the controller module.
- b. Press down on the orange tab on top of the latching mechanism until it clears the latching pin on the chassis.

The latching mechanism hook should be nearly vertical and should be clear of the chassis pin.

- c. Gently pull the controller module a few inches toward you so that you can grasp the controller module sides.
- d. Using both hands, gently pull the controller module out of the chassis and set it on a flat, stable surface.

## Step 2: Replace the boot media

You must locate the boot media in the controller module, and then follow the directions to replace it.

1. Open the air duct and locate the boot media using the following illustration or the FRU map on the controller module:
2. Locate and remove the boot media from the controller module:



- a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
- b. Rotate the boot media up and gently pull the boot media out of the socket.

1. 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.

3. Lock the boot media in place:

- a. Rotate the boot media down toward the motherboard.
- b. 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.
- c. While pushing down on the boot media, lift the blue locking button to lock the boot media in place.

4. Close the air duct.

### Step 3: Transfer the boot image to the boot media using a USB flash drive

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.

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

- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.
1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
    - 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 reinstallation of the controller module:
  - a. Make sure the latch arms are locked in the extended position.
  - b. Using the latch arms, push the controller module into the chassis bay until it stops.



Do not push down on the latching mechanism at the top of the latch arms. Doing so will raise the locking mechanism and prohibit sliding the controller module into the chassis.

- c. Press down and hold the orange tabs on top of the latching mechanism.
- d. Gently push the controller module into the chassis bay until it is flush with the edges of the chassis.



The latching mechanism arms slide into the chassis.

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

- e. Release the latches to lock the controller module into place.
- f. 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. 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 node that is displayed on the screen.
  - b. Press `y` when prompted to restore the backup configuration.

- c. Press `y` when prompted to overwrite `/etc/ssh/ssh_host_dsa_key`.
13. From the partner node 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`
14. If the restore is successful, press `y` on the impaired node when prompted to use the restored copy?.
15. Press `y` when you see confirm backup procedure was successful, and then press `y` when prompted to reboot the node.
16. Verify that the environmental variables are set as expected.
  - a. Take the node 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 node.
17. With the rebooted impaired node displaying the `Waiting for giveback...` message, perform a giveback from the healthy node:

If your system is in...	Then...
An HA pair	<p>After the impaired node is displaying the <code>Waiting for giveback...</code> message, perform a giveback from the healthy node:</p> <ol style="list-style-type: none"> <li>a. From the healthy node: <code>storage failover giveback -ofnode partner_node_name</code></li> </ol> <p>The impaired node takes back its storage, finishes booting, and then reboots and is again taken over by the healthy node.</p> <div style="display: flex; align-items: center;">  <p>If the giveback is vetoed, you can consider overriding the vetoes.</p> </div> <p><a href="#">ONTAP 9 High-Availability Configuration Guide</a></p> <ol style="list-style-type: none"> <li>b. Monitor the progress of the giveback operation by using the <code>storage failover show-giveback</code> command.</li> <li>c. After the giveback operation is complete, confirm that the HA pair is healthy and that takeover is possible by using the <code>storage failover show</code> command.</li> <li>d. Restore automatic giveback if you disabled it using the <code>storage failover modify</code> command.</li> </ol>

18. Exit advanced privilege level on the healthy node.

# Boot the recovery image - AFF A320

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

If your system has...	Then...
No network connection and is in a MetroCluster IP configuration	<p>a. Press <b>n</b> when prompted to restore the backup configuration.</p> <p>b. Reboot the system when prompted by the system.</p> <p>c. Wait for the iSCSI storage connections to connect.</p> <p>You can proceed after you see the following messages:</p> <div data-bbox="672 394 1489 1257" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> 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).</pre> </div> <p>d. Select the <b>Update flash from backup config</b> (sync flash) option from the displayed menu.</p> <p>If you are prompted to continue with the update, press <b>y</b>.</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 [Post boot media replacement steps for OKM, NSE, and NVE](#)

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

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.

## Restore OKM, NSE, and NVE as needed - AFF A320

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

- 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+wAAAAAAAA
lgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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...	<ol style="list-style-type: none"> <li>a. Log into the partner node.</li> <li>b. Confirm the target node is ready for giveback with the <code>storage failover show</code> command.</li> </ol>

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 A320

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.