



# Boot media

## Install and maintain

NetApp  
February 13, 2026

# Table of Contents

- Boot media ..... 1
  - Overview of boot media replacement - AFF A300 ..... 1
  - Check encryption key support and status - AFF A300 ..... 1
    - Step 1: Check NVE support and download the correct ONTAP image ..... 1
    - Step 2: Verify key manager status and back up configuration ..... 2
  - Shut down the impaired controller - AFF A300 ..... 4
    - Option 1: Most configurations ..... 4
    - Option 2: Controller is in a MetroCluster configuration ..... 5
    - Option 3: Controller is in a two-node MetroCluster ..... 6
  - Replace the boot media - AFF A300 ..... 8
    - Step 1: Remove the controller module ..... 8
    - Step 2: Replace the boot media - AFF A300 ..... 9
    - Step 3: Transfer the boot image to the boot media ..... 10
  - Boot the recovery image - AFF A300 ..... 12
    - Option 1: Most systems ..... 12
    - Option 2: Controller is in a two-node MetroCluster ..... 14
  - Switch back aggregates in a two-node MetroCluster configuration - AFF A300 ..... 14
  - Restore encryption - AFF A300 ..... 16
  - Return the failed part to NetApp - AFF A300 ..... 26

# Boot media

## Overview of boot media replacement - AFF A300

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 encryption key support and status - AFF A300

To ensure data security on your storage system, you need to verify the encryption key support and status on your boot media. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Check if your ONTAP version supports NetApp Volume Encryption (NVE), and before you shut down the controller check if the key manager is active.

### Step 1: Check NVE support and download the correct ONTAP image

Determine whether your ONTAP version supports NetApp Volume Encryption (NVE) so you can download the correct ONTAP image for the boot media replacement.

#### Steps

1. Check if your ONTAP version supports encryption:

```
version -v
```

If the output includes `1Ono-DARE`, NVE is not supported on your cluster version.

2. Download the appropriate ONTAP image based on NVE support:

- If NVE is supported: Download the ONTAP image with NetApp Volume Encryption
- If NVE is not supported: Download the ONTAP image without NetApp Volume Encryption



Download the ONTAP image from the NetApp Support Site to your HTTP or FTP server or a local folder. You will need this image file during the boot media replacement procedure.

## Step 2: Verify key manager status and back up configuration

Before shutting down the impaired controller, verify the key manager configuration and back up the necessary information.

### Steps

1. Determine which key manager is enabled on your system:

ONTAP version	Run this command
ONTAP 9.14.1 or later	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"> <li>• If EKM is enabled, <code>EKM</code> is listed in the command output.</li> <li>• If OKM is enabled, <code>OKM</code> is listed in the command output.</li> <li>• If no key manager is enabled, <code>No key manager keystores configured</code> is listed in the command output.</li> </ul>
ONTAP 9.13.1 or earlier	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> <li>• If EKM is enabled, <code>external</code> is listed in the command output.</li> <li>• If OKM is enabled, <code>onboard</code> is listed in the command output.</li> <li>• If no key manager is enabled, <code>No key managers configured</code> is listed in the command output.</li> </ul>

2. Depending on whether a key manager is configured on your system, do one of the following:

#### If no key manager is configured:

You can safely shut down the impaired controller and proceed to the shutdown procedure.

#### If a key manager is configured (EKM or OKM):

- a. Enter the following query command to display the status of the authentication keys in your key manager:

```
security key-manager key query
```

- b. Review the output and check the value in the `Restored` column. This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Complete the appropriate procedure based on your key manager type:

### External Key Manager (EKM)

Complete these steps based on the value in the `Restored` column.

#### If all keys show `true` in the `Restored` column:

You can safely shut down the impaired controller and proceed to the shutdown procedure.

#### If any keys show a value other than `true` in the `Restored` column:

- 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 all authentication keys are restored:

```
security key-manager key query
```

Confirm that the `Restored` column displays `true` for all authentication keys.

- c. If all keys are restored, you can safely shut down the impaired controller and proceed to the shutdown procedure.

### Onboard Key Manager (OKM)

Complete these steps based on the value in the `Restored` column.

#### If all keys show `true` in the `Restored` column:

- a. Back up the OKM information:

- i. Switch to advanced privilege mode:

```
set -priv advanced
```

Enter `y` when prompted to continue.

- ii. Display the key management backup information:

```
security key-manager onboard show-backup
```

- iii. Copy the backup information to a separate file or your log file.

You will need this backup information if you need to manually recover OKM during the replacement procedure.

- iv. Return to admin mode:

```
set -priv admin
```

- b. You can safely shut down the impaired controller and proceed to the shutdown procedure.

#### If any keys show a value other than `true` in the `Restored` column:

a. Synchronize the onboard key manager:

```
security key-manager onboard sync
```

Enter the 32-character alphanumeric onboard key management passphrase when prompted.



This is the cluster-wide passphrase you created when you initially configured the Onboard Key Manager. If you do not have this passphrase, contact NetApp Support.

b. Verify all authentication keys are restored:

```
security key-manager key query
```

Confirm that the `Restored` column displays `true` for all authentication keys and the `Key Manager type` shows `onboard`.

c. Back up the OKM information:

i. Switch to advanced privilege mode:

```
set -priv advanced
```

Enter `y` when prompted to continue.

ii. Display the key management backup information:

```
security key-manager onboard show-backup
```

iii. Copy the backup information to a separate file or your log file.

You will need this backup information if you need to manually recover OKM during the replacement procedure.

iv. Return to admin mode:

```
set -priv admin
```

d. You can safely shut down the impaired controller and proceed to the shutdown procedure.

## Shut down the impaired controller - AFF A300

Shut down or take over the impaired controller using the appropriate procedure for your configuration. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

### Option 1: Most configurations

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

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

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

### Steps

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

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

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
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 controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name</pre> <p>When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <code>y</code>.</p>

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

#### About this task

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

#### Steps

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

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <pre>metrocluster switchover</pre>
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.

- 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:

```
mccl1A::> 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 A300

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. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

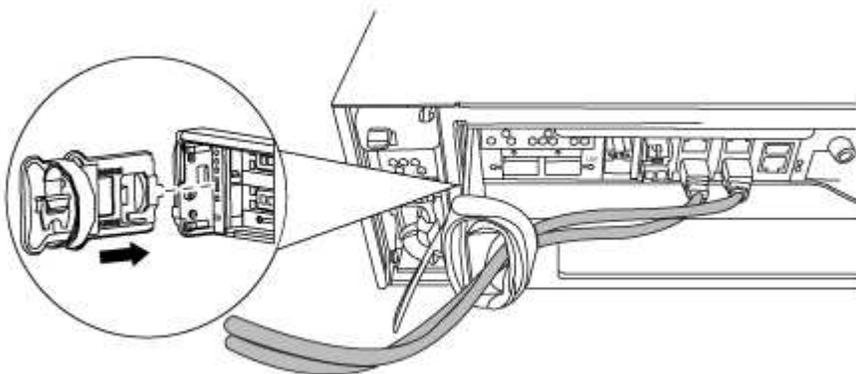
### Step 1: Remove the controller module

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

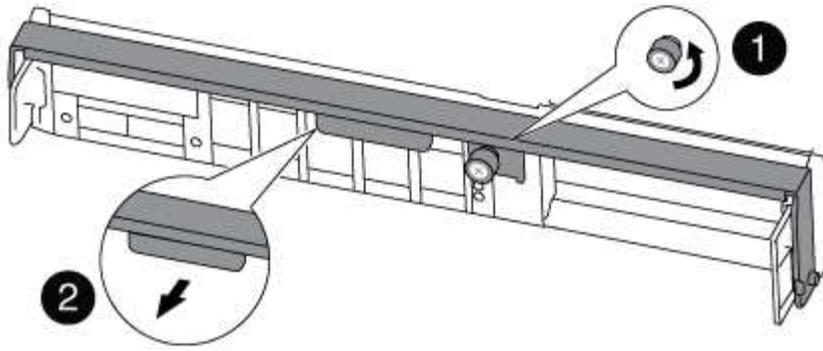
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

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

3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Loosen the thumbscrew on the cam handle on the controller module.



1	Thumbscrew
2	Cam handle

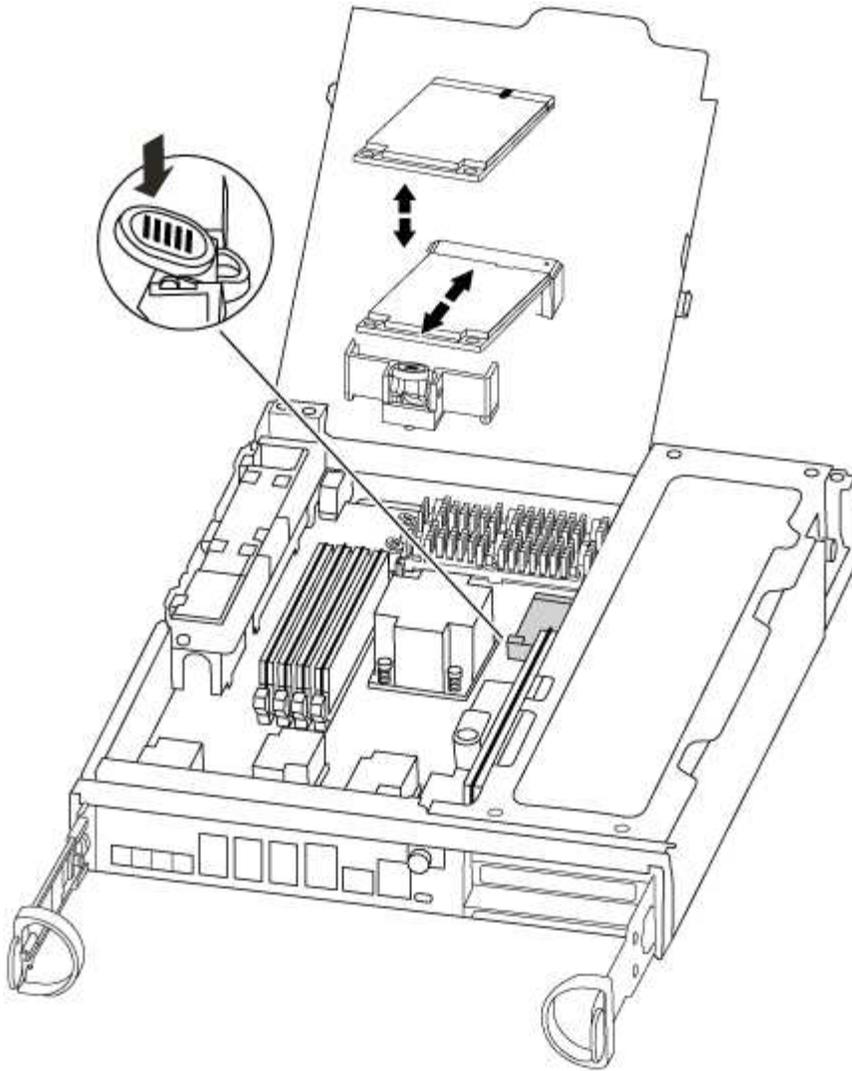
5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

## Step 2: Replace the boot media - AFF A300

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

1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:



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



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

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

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

### Step 3: Transfer the boot image to the boot media

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

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is 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. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

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

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

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

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

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

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

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

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

The system begins to boot and stops at the LOADER prompt.

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

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



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

- If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
  - `filer_addr` is the IP address of the storage system.
  - `netmask` is the network mask of the management network that is connected to the HA partner.

- gateway is the gateway for the network.
- dns\_addr is the IP address of a name server on your network.
- dns\_domain is the Domain Name System (DNS) domain name.

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



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

8. 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 A300

The procedure for booting the impaired controller from the recovery image depends on whether the system is in a two-controller MetroCluster configuration. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

### 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.

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>Press <code>y</code> when prompted to restore the backup configuration.</li> <li>Set the healthy controller to advanced privilege level: <code>set -privilege advanced</code></li> <li>Run the restore backup command: <code>system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code></li> <li>Return the controller to admin level: <code>set -privilege admin</code></li> <li>Press <code>y</code> when prompted to use the restored configuration.</li> <li>Press <code>y</code> when prompted to reboot the controller.</li> </ol>
No network connection	<ol style="list-style-type: none"> <li>Press <code>n</code> when prompted to restore the backup configuration.</li> <li>Reboot the system when prompted by the system.</li> <li>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>

- Ensure that the environmental variables are set as expected:
  - Take the controller 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.
  - Save your changes using the `savenv` command.
- 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.
- 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 controller.</li> <li>Confirm the target controller is ready for giveback with the <code>storage failover show</code> command.</li> </ol>

- 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.

## 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

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

The image is downloaded from the USB flash drive.

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

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

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.
5. Verify that the environmental variables are set as expected.
  - a. Take the node to the LOADER prompt.
  - b. Check the environment variable settings with the `printenv` command.
  - c. If an environment variable is not set as expected, modify it with the `setenv environment-variable-name changed-value` command.
  - d. Save your changes using the `savenv` command.
  - e. Reboot the node.

## Switch back aggregates in a two-node MetroCluster configuration - AFF A300

After completing the boot media replacement, perform the MetroCluster switchback operation. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

This task only applies to two-node MetroCluster configurations.

## Steps

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

```
cluster_B::> metrocluster node show

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

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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

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

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

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

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using

the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

## Restore encryption - AFF A300

Restore encryption on the replacement boot media. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Complete the appropriate steps to restore encryption on your system based on your key manager type. If you are unsure which key manager your system uses, check the settings you captured at the beginning of the boot media replacement procedure.

## Onboard Key Manager (OKM)

Restore the Onboard Key Manager (OKM) configuration from the ONTAP boot menu.

### Before you begin

Ensure you have the following information available:

- Cluster-wide passphrase entered while [enabling onboard key management](#)
- [Backup information for the Onboard Key Manager](#)
- Verification that you have the correct passphrase and backup data using the [How to verify onboard key management backup and cluster-wide passphrase](#) procedure

### Steps

#### On the impaired controller:

1. Connect the console cable to the impaired controller.
2. From the ONTAP boot menu, select the appropriate option:

ONTAP version	Select this option
ONTAP 9.8 or later	<p>Select option 10.</p> <p><b>Show example boot menu</b></p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"><p>Please choose one of the following:</p><ul style="list-style-type: none"><li>(1) Normal Boot.</li><li>(2) Boot without /etc/rc.</li><li>(3) Change password.</li><li>(4) Clean configuration and initialize all disks.</li><li>(5) Maintenance mode boot.</li><li>(6) Update flash from backup config.</li><li>(7) Install new software first.</li><li>(8) Reboot node.</li><li>(9) Configure Advanced Drive Partitioning.</li><li>(10) Set Onboard Key Manager recovery secrets.</li><li>(11) Configure node for external key management.</li></ul><p>Selection (1-11)? 10</p></div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p data-bbox="634 155 1377 191">Select the hidden option <code>recover_onboard_keymanager</code></p> <p data-bbox="634 226 959 262"><b>Show example boot menu</b></p> <div data-bbox="667 304 1422 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p data-bbox="695 338 1305 369">Please choose one of the following:</p> <ul style="list-style-type: none"> <li data-bbox="699 417 987 449">(1) Normal Boot.</li> <li data-bbox="699 457 1146 489">(2) Boot without <code>/etc/rc</code>.</li> <li data-bbox="699 497 1057 529">(3) Change password.</li> <li data-bbox="695 537 1377 606">(4) Clean configuration and initialize all disks.</li> <li data-bbox="699 615 1162 646">(5) Maintenance mode boot.</li> <li data-bbox="699 655 1338 686">(6) Update flash from backup config.</li> <li data-bbox="699 695 1252 726">(7) Install new software first.</li> <li data-bbox="699 735 987 766">(8) Reboot node.</li> <li data-bbox="695 774 1203 844">(9) Configure Advanced Drive Partitioning.</li> </ul> <p data-bbox="695 852 992 884">Selection (1-19)?</p> <p data-bbox="695 892 1149 924"><code>recover_onboard_keymanager</code></p> </div>

3. Confirm that you want to continue the recovery process when prompted:

**Show example prompt**

```
This option must be used only in disaster recovery procedures. Are you
sure? (y or n):
```

4. Enter the cluster-wide passphrase twice.

While entering the passphrase, the console does not show any input.

**Show example prompt**

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
```

5. Enter the backup information:

- a. Paste the entire content from the BEGIN BACKUP line through the END BACKUP line, including the dashes.



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
-----END
BACKUP-----
```

b. Press Enter twice at the end of the input.

The recovery process completes and displays the following message:

Successfully recovered keymanager secrets.

### Show example prompt

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*****
*****
* Select option "(1) Normal Boot." to complete recovery
process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*****
*****
```



Do not proceed if the displayed output is anything other than Successfully recovered keymanager secrets. Perform troubleshooting to correct the error.

6. Select option 1 from the boot menu to continue booting into ONTAP.

### Show example prompt

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Confirm that the controller's console displays the following message:

```
Waiting for giveback...(Press Ctrl-C to abort wait)
```

#### **On the partner controller:**

8. Giveback the impaired controller:

```
storage failover giveback -fromnode local -only-cfo-aggregates true
```

#### **On the impaired controller:**

9. After booting with only the CFO aggregate, synchronize the key manager:

```
security key-manager onboard sync
```

10. Enter the cluster-wide passphrase for the Onboard Key Manager when prompted.

## Show example prompt

```
Enter the cluster-wide passphrase for the Onboard Key Manager:
```

```
All offline encrypted volumes will be brought online and the corresponding volume encryption keys (VEKs) will be restored automatically within 10 minutes. If any offline encrypted volumes are not brought online automatically, they can be brought online manually using the "volume online -vserver <vserver> -volume <volume_name>" command.
```



If the sync is successful, the cluster prompt is returned with no additional messages. If the sync fails, an error message appears before returning to the cluster prompt. Do not continue until the error is corrected and the sync runs successfully.

11. Verify that all keys are synced:

```
security key-manager key query -restored false
```

The command should return no results. If any results appear, repeat the sync command until no results are returned.

### On the partner controller:

12. Giveback the impaired controller:

```
storage failover giveback -fromnode local
```

13. Restore automatic giveback if you disabled it:

```
storage failover modify -node local -auto-giveback true
```

14. If AutoSupport is enabled, restore automatic case creation:

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

## External Key Manager (EKM)

Restore the External Key Manager configuration from the ONTAP boot menu.

### Before you begin

Gather the following files from another cluster node or from your backup:

- /cfcard/knip/servers.cfg file or the KMIP server address and port
- /cfcard/knip/certs/client.crt file (client certificate)
- /cfcard/knip/certs/client.key file (client key)
- /cfcard/knip/certs/CA.pem file (KMIP server CA certificates)

## Steps

### On the impaired controller:

1. Connect the console cable to the impaired controller.
2. Select option 11 from the ONTAP boot menu.

#### Show example boot menu

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 11
```

3. Confirm you have gathered the required information when prompted:

#### Show example prompt

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

4. Enter the client and server information when prompted:
  - a. Enter the client certificate (client.crt) file contents, including the BEGIN and END lines.
  - b. Enter the client key (client.key) file contents, including the BEGIN and END lines.
  - c. Enter the KMIP server CA(s) (CA.pem) file contents, including the BEGIN and END lines.
  - d. Enter the KMIP server IP address.
  - e. Enter the KMIP server port (press Enter to use the default port 5696).

### Show example

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

The recovery process completes and displays the following message:

```
Successfully recovered keymanager secrets.
```

### Show example

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Select option 1 from the boot menu to continue booting into ONTAP.

### Show example prompt

```
*****  
*****  
* Select option "(1) Normal Boot." to complete the recovery  
process.  
*  
*****  
*****  
  
(1) Normal Boot.  
(2) Boot without /etc/rc.  
(3) Change password.  
(4) Clean configuration and initialize all disks.  
(5) Maintenance mode boot.  
(6) Update flash from backup config.  
(7) Install new software first.  
(8) Reboot node.  
(9) Configure Advanced Drive Partitioning.  
(10) Set Onboard Key Manager recovery secrets.  
(11) Configure node for external key management.  
Selection (1-11)? 1
```

#### 6. Restore automatic giveback if you disabled it:

```
storage failover modify -node local -auto-giveback true
```

#### 7. If AutoSupport is enabled, restore automatic case creation:

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

## Return the failed part to NetApp - AFF A300

Return the failed part to NetApp after replacing the boot media. The AFF A300 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

## Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.