Boot media

Install and maintain

NetApp
February 01, 2026

Table of Contents

Boot media

Boot media replacement workflow - AFX 1K

Get started with replacing the boot media in your AFX 1K storage system by reviewing the replacement requirements, checking encryption status, shutting down the controller, replacing the boot media, booting the recovery image, restoring encryption, and verifying the system functionality.

1. **Review the boot media requirements**

Review the requirements for boot media replacement.

2. **Shut down the controller**

Shut down the controller in your storage system when you need to replace the boot media.

3. **Replace the boot media**

Remove the failed boot media from the System Management module and install the replacement boot media.

4. **Restore the image on the boot media**

Restore the ONTAP image from the partner controller.

5. **Return the failed part to NetApp**

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Requirements to replace the boot media - AFX 1K

Before replacing the boot media in your AFX 1K storage system, ensure you meet the necessary requirements for a successful replacement. This includes verifying that you have the correct replacement boot media, confirming that there are no defective cluster ports on the controller, and determining whether Onboard Key Manager (OKM) or External Key Manager (EKM) is enabled.

Before replacing the boot media, make sure to review the following requirements.

- 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.

- There must be no faulty cluster ports on the impaired controller.

What's next?

After you've reviewed the requirements to replace the boot media, you need to shut down the controller.

Shut down the controller to replace the boot media - AFX 1K

Shut down the impaired controller in your AFX 1K storage system to prevent data loss and ensure system stability when replacing the boot media.

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

About this task

- If you have a cluster with more than four nodes, it must be in quorum. To view cluster information about your nodes, use the `cluster show` command. For more information about the `cluster show` command, see View node-level details in an ONTAP cluster.
- If the cluster is not in quorum or if the health or eligibility of any controller (other than the impaired controller) shows as false, you must correct the issue before shutting down the impaired controller. See Synchronize a node with the cluster.

Steps

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

   ```
   system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
   ```

   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 impaired controller:

   ```
   storage failover modify -node impaired-node -auto-giveback-of false
   ```

   When you see *Do you want to disable auto-giveback?*, enter `y`.

   a. If you are running ONTAP version 9.17.1 and the impaired controller cannot be brought up or is already taken over, you must take the HA interconnect link down from the healthy controller before booting up the impaired controller. This prevents the impaired controller from performing automatic giveback.

      ```
      system ha interconnect link off -node healthy-node -link 0
      ```

      ```
      system ha interconnect link off -node healthy-node -link 1
      ```

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name -halt true` The *-halt true* parameter brings the impaired node to the LOADER prompt.

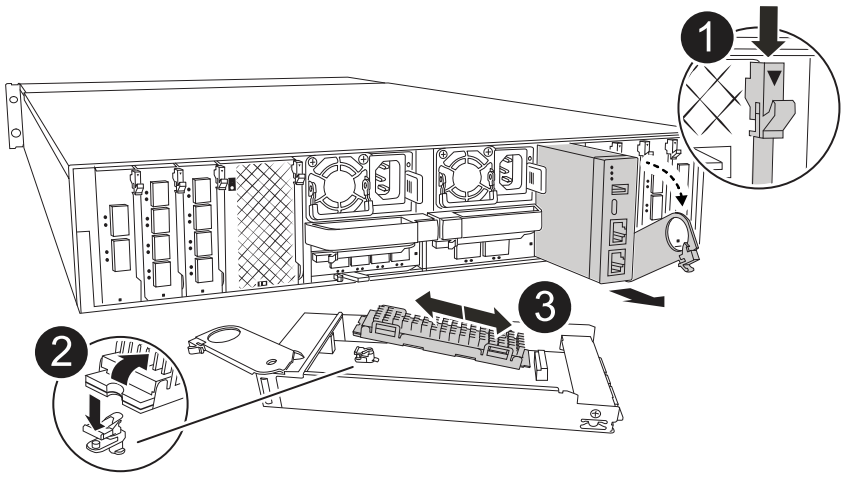
What's next?

After shutting down the controller, change the boot media.

Replace the boot media - AFX 1K

The boot media in your AFX 1K storage system stores essential firmware and configuration data. The replacement process involves removing the System Management module, removing the impaired boot media, installing the replacement boot media in the System Management module, and then reinstalling the System Management module.

The boot media is located inside the System Management module and is accessed by removing the module from the system.



1	System Management module cam latch
2	Boot media locking button
3	Boot media

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the power supply cables from the PSUs.
3. Remove the System Management module:
    a. Remove cables from the System Management module and label them to ensure correct reconnection during reinstallation.
    b. Rotate the cable management tray down by pulling the buttons on both sides on the inside of the cable management tray and then rotate the tray down.
    c. Depress the System Management cam button.
    d. Rotate the cam latch down as far as it will go.
    e. Remove the System Management module from the enclosure by hooking your finger into the cam lever opening and pulling the module out of the enclosure.
    f. Place the System Management module on an anti-static mat, so that the boot media is accessible.
4. Remove the boot media from the management module:
    a. Press the blue locking button.
    b. Rotate the boot media up, slide it out of the socket, and set it aside.
5. Install the replacement boot media into the System Management module:
    a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.
    b. Rotate the boot media down toward the locking button.
    c. Push the locking button, rotate the boot media all the way down and then release the locking button.
6. Reinstall the System Management module:
    a. Align the module with the edges of the enclosure slot opening.
    b. Gently slide the module into the slot all the way into the enclosure, and then rotate the cam latch all the way up to lock the module in place.
7. Rotate the cable management tray up to the closed position.
    a. Recable the System Management module.
8. Plug the power cables into the power supplies and reinstall the power cable retainer.

    The controller begins to boot as soon as power is reconnected to the system.

What's next?

After replacing the boot media, restore the ONTAP image from the partner node.

Boot the recovery image - AFX 1K

After installing the new boot media device in your AFX 1K storage system, you can start the automated boot media recovery process to restore the configuration from the partner node.

About this task

During the recovery process, the system checks whether encryption is enabled and identifies the type of key encryption being used. If key encryption is enabled, the system guides you through the appropriate steps to

restore it.

Before you begin

- For OKM, you need the cluster-wide passphrase and the backup data.
- For EKM, you need copies of the following files from the partner node:
  - /cfcard/kmip/servers.cfg file.
  - /cfcard/kmip/certs/client.crt file.
  - /cfcard/kmip/certs/client.key file.
  - /cfcard/kmip/certs/CA.pem file.

Steps

1. From the LOADER prompt, enter the command:

   ```
   boot_recovery -partner
   ```

   The screen displays the following message:

   ```
   Starting boot media recovery (BMR) process. Press Ctrl-C to abort…
   ```

2. Monitor the boot media install recovery process.

   The process completes and displays the `Installation complete` message.

3. The system checks for encryption and encryption type and displays one of two messages. Depending on what message is displayed, take one of the following actions:

   Occasionally, the process may not be able to identify if key manager is configured on the system. It will display an error message, ask if key manager is configured for the system, and then ask what type of key manager is configured. The process will resume after you resolve the issue.

   Show example of configuration error finding prompts

   ```
   Error when fetching key manager config from partner ${partner_ip}:
   ${status}

   Has key manager been configured on this system

   Is the key manager onboard
   ```

If you see this message…	Do this…
`key manager is not configured. Exiting.`	Encryption is not configured on the system. Complete the following steps: a. Press <enter> when console messages stop. ◦ If you see the login prompt, go to step 4. ◦ If you do not see login prompt, log into the partner node and proceed to step 4. b. Go to step 6 to enable automatic giveback if it was disabled.
`key manager is configured.`	Go to step 5 to restore the appropriate key manager. The node accesses the boot menu and runs: • Option 10 for systems with Onboard Key Manager (OKM). • Option 11 for systems with External Key Manager (EKM).

4. If encryption is not installed on the system and the login prompt is not displayed. Complete the following steps:
   a. Give back only the root with override-destination-checks option:

      ```
      storage failover giveback -ofnode impaired-node -only-root true -override -destination-checks true
      ```

      This command is available only in Diagnostic mode. For details, see Privilege levels for ONTAP CLI commands.

      If you encounter errors, contact NetApp Support.

   b. Wait 5 minutes after the giveback report completes, and check failover status and giveback status:

      `storage failover show` and `storage failover show-giveback`

      The following command is only available in the Diagnostic mode privilege level.

   c. If you are running ONTAP 9.17.1 and the HA internconnect links were taken down, bring them back up:

      ```
      system ha interconnect link on -node healthy-node -link 0

      system ha interconnect link on -node healthy-node -link 1
      ```

      If you are running 9.18.1 or higher, skip the above step and go to the next step.

   d. Return the impaired controller to normal operation by giving back its storage:

      `storage failover giveback -ofnode` *`impaired_node_name`*

5. For systems with key-manager configured, select the appropriate key manager restoration process.

Onboard Key Manager (OKM)

If OKM is detected, the system displays the following message and begins running BootMenu Option 10.

```
key manager is configured.
Entering Bootmenu Option 10...

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

a. Enter `Y` at the prompt to confirm you want to start the OKM recovery process.

b. Enter the following when prompted:

   i. The passphrase

   ii. The passphrase again when prompted to confirm

   iii. Backup data for onboard key manager

   Show example of passphrase and backup data prompts

   ```
   Enter the passphrase for onboard key management:
   -----BEGIN PASSPHRASE-----
   <passphrase_value>
   -----END PASSPHRASE-----
   Enter the passphrase again to confirm:
   -----BEGIN PASSPHRASE-----
   <passphrase_value>
   -----END PASSPHRASE-----
   Enter the backup data:
   -----BEGIN BACKUP-----
   <passphrase_value>
   -----END ACKUP-----
   ```

c. Continue to monitor the recovery process as it restores the appropriate files from the partner node.

   When the recovery process is complete, the node will reboot. The following messages indicate a successful recovery:

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

Successfully recovered keymanager secrets.
```

d. When the node reboots, verify the boot media recovery was successful by confirming that the system is back online and operational.

e. Return the impaired controller to normal operation by giving back its storage:

```
storage failover giveback -ofnode impaired_node_name
```

i. If the HA interconnect links were taken down, bring them back up to resume automatic giveback:

```
system ha interconnect link on -node healthy-node -link 0

system ha interconnect link on -node healthy-node -link 1
```

f. After the partner node is fully up and serving data, synchronize the OKM keys across the cluster.

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

External Key Manager (EKM)

If EKM is detected, the system displays the following message and begins running BootMenu Option 11.

```
key manager is configured.
Entering Bootmenu Option 11...
```

a. Depending on whether the key is successfully restored, take one of the following actions:

- If you see `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` in the output, the EKM configuration has been successfully restored.

  The process attempts to restore the appropriate files from the partner node and reboots the node. Continue to the next step.

- If the key is not successfully restored, the system will halt and indicate that it could not restore the key. The error and warning messages are displayed. You must rerun the recovery process:

  ```
  boot_recovery -partner
  ```

Show example of key recovery error and warning messages

```
ERROR: kmip_init: halting this system with encrypted
mroot...
WARNING: kmip_init: authentication keys might not be
available.
*****************************************************
*                 A T T E N T I O N                 *
*                                                   *
*       System cannot connect to key managers.      *
*                                                   *
*****************************************************
ERROR: kmip_init: halting this system with encrypted
mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

b. When the node reboots, verify that the boot media recovery was successful by confirming that the system is back online and operational.

c. Return the controller to normal operation by giving back its storage:

```
storage failover giveback -ofnode impaired_node_name
```

i. If the HA interconnect links were taken down, bring them back up to resume automatic giveback:

```
system ha interconnect link on -node healthy-node -link 0
```

```
system ha interconnect link on -node healthy-node -link 1
```

6. If automatic giveback was disabled, reenable it:

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

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

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

What's next?

After you've restored the ONTAP image and the node is up and serving data, you need to return the failed part

to NetApp.

Return the failed part to NetApp - AFX 1K

If a component in your AFX 1K storage system fails, return the failed part to NetApp. See the Part Return and Replacements page for further information.

Copyright information

Trademark information