



# Boot media

## Install and maintain

NetApp  
October 30, 2024

# Table of Contents

- Boot media ..... 1
  - Boot media replacement workflow - FAS70 and FAS90 ..... 1
  - Boot media replace requirements - FAS70 and FAS90 ..... 1
  - Check encryption key support and status - FAS70 and FAS90 ..... 2
  - Shut down the impaired controller - FAS70 and FAS90 ..... 5
  - Replace the boot media - FAS70 and FAS90 ..... 7
  - Boot the recovery image - FAS70 and FAS90 ..... 10
  - Restore encryption - FAS70 and FAS90 ..... 11
  - Return the failed part to NetApp - FAS70 and FAS90 ..... 20

# Boot media

## Boot media replacement workflow - FAS70 and FAS90

Follow these workflow steps to replace your boot media.

1

### Review boot media replacement requirements

To replace the boot media, you must meet certain requirements.

2

### Check onboard encryption keys

Verify whether the system has security key manager enabled or encrypted disks.

3

### Shut down the impaired controller

Shut down or take over the impaired controller so that the healthy controller continues to serve data from the impaired controller storage.

4

### Replace the boot media

Remove the failed boot media from the System Management module and install the replacement boot media, and then transfer an ONTAP image using a USB flash drive to the replacement boot media.

5

### Boot the recovery image

Boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables..

6

### Restore encryption

Restore the onboard key manager configuration or the external key manager from the ONATP boot menu.

7

### Return the failed part to NetApp

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

## Boot media replace requirements - FAS70 and FAS90

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

- You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz` file.
- You must copy the `image_xxx.tgz` file to the USB flash drive for later use in this procedure.
- You must replace the failed component with a replacement FRU component you received NetApp.

- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

## Check encryption key support and status - FAS70 and FAS90

Before shutting down the impaired controller, check if your version of ONTAP supports NetApp Volume Encryption (NVE) and if your key management system is properly configured.

### Step 1: Check if your version of ONTAP supports NetApp Volume Encryption

Check whether your ONTAP version supports NetApp Volume Encryption (NVE). This information is crucial for downloading the correct ONTAP image.

1. Determine if your ONTAP version supports encryption by running the following command:

```
version -v
```

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

2. Depending on whether NVE is supported on your system, take one of the following actions:
  - 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.

### Step 2: Determine if it is safe to shut down the controller

To safely shut down a controller, first identify whether the External Key Manager (EKM) or the Onboard Key Manager (OKM) is active. Then, verify the key manager in use, display the appropriate key information, and take action based on the status of the authentication keys.

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 version	Run this command
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 manger is configured on your system, select one of the following options.

**No key manager configured**

You can safely shut down the impaired controller. Go to [shutdown the impaired controller](#).

**External or Onboard key manager configured**

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

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

- b. Check the output for the value in the `Restored` column for your key manager.

This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Depending on whether you're system is using the External Key Manager or Onboard Key Manager, select one of the following options.

## External Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
<code>true</code>	You can safely shut down the impaired controller. Go to <a href="#">shutdown the impaired controller</a> .
Anything other than <code>true</code>	<ol style="list-style-type: none"><li>Restore the external key management authentication keys to all nodes in the cluster using the following command: <pre>security key-manager external restore</pre><p>If the command fails, contact <a href="#">NetApp Support</a>.</p></li><li>Verify that the <code>Restored</code> column displays <code>true</code> for all authentication keys by entering the <code>security key-manager key query</code> command.  If all the authentication keys are <code>true</code>, you can safely shut down the impaired controller. Go to <a href="#">shutdown the impaired controller</a>.</li></ol>

## Onboard Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
<code>true</code>	<p>Manually back up the OKM information.</p> <ol style="list-style-type: none"><li>Go to the advanced mode by entering <code>set -priv advanced</code> and then enter <code>Y</code> when prompted.</li><li>Enter the following command to display the key management information: <pre>security key-manager onboard show-backup</pre></li><li>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.</li><li>You can safely shut down the impaired controller. Go to <a href="#">shutdown the impaired controller</a>.</li></ol>

Output value in Restored column	Follow these steps...
Anything other than <code>true</code>	<p>a. Enter the onboard security key-manager sync command:</p> <pre>security key-manager onboard sync</pre> <p>b. Enter the 32 character, alphanumeric onboard key management passphrase when prompted.</p> <p>If the passphrase cannot be provided, contact <a href="#">NetApp Support</a>.</p> <p>c. Verify the Restored column displays <code>true</code> for all authentication keys:</p> <pre>security key-manager key query</pre> <p>d. Verify that the Key Manager type displays <code>onboard</code>, and then manually back up the OKM information.</p> <p>e. Enter the command to display the key management backup information:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>g. You can safely shut down the impaired controller. Go to <a href="#">shutdown the impaired controller</a>.</p>

## Shut down the impaired controller - FAS70 and FAS90

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller. Shut down or take over the impaired controller using the appropriate procedure for your configuration.

## Option 1: Most systems

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.

### About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for the impaired controller SCSI blade. The `cluster kernel-service show` command (from `priv advanced` mode) displays the node name, [quorum status](#) of that node, availability status of that node, and operational status of that node.

Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- 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](#).

### 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 healthy controller: `storage failover modify -node local -auto-giveback false`



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

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

## Option 2: Controller is in a MetroCluster

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](#).
- 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:

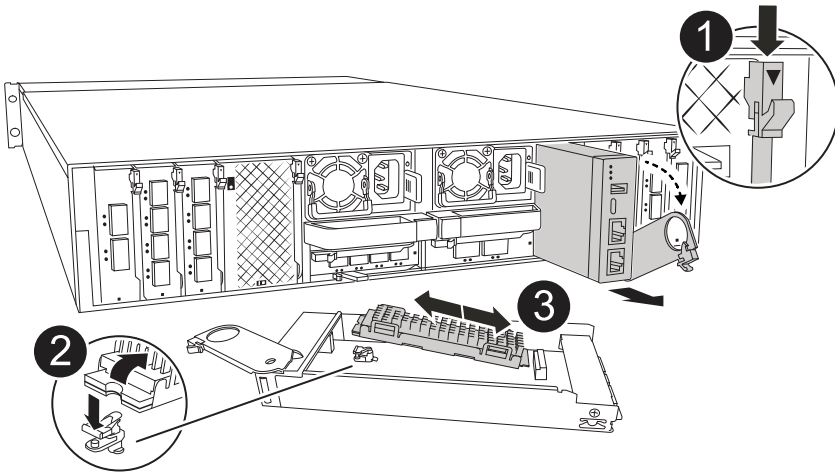
If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next section.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: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

## Replace the boot media - FAS70 and FAS90

You must unplug the controller module, remove the System Management module from the back of the system, remove the impaired boot media, and install the replacement boot media in the System Management module.

### Step 1: Replace the boot media

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

1. If you are not already grounded, properly ground yourself.
2. Unplug the power supply cables from the PSUs from the controller.



If your storage system has DC power supplies, disconnect the power cable block from the power supply units (PSUs).

- a. Remove any cables connected to the System Management module. Make sure that you label where the cables were connected, so that you can connect them to the correct ports when you reinstall the module.
  - 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.
3. 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.
  4. 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.

5. 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.
6. Rotate the cable management tray up to the closed position.
  - a. Recable the System Management module.

## Step 2: Transfer the ONTAP image to the boot media

The replacement boot media that you installed is without an ONTAP image. You can transfer the ONTAP image to the replacement boot media by downloading the appropriate ONTAP service image from the [NetApp Support Site](#) to a USB flash drive and then to the replacement boot media.

### Before you begin

- You must have an empty USB flash drive, formatted to FAT32, with at least 4GB capacity.
- Download 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. Use the `version -v` command to display if your version of ONTAP supports NVE. If the command output displays `<10no- DARE>`, your version of ONTAP does not support NVE.
  - If NVE is supported by your version of ONTAP, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not supported, 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 between the node management ports of the controllers (typically the e0M interfaces).

### Steps

1. Download and copy the appropriate service image from the [NetApp Support Site](#) to the USB flash drive.
  - a. Download the service image from the Downloads link on the page, 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.

The USB flash drive should have the appropriate ONTAP image of what the impaired controller is running.

- c. Remove the USB flash drive from your laptop.
2. Insert the USB flash drive into the USB slot on the System Management module.

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

3. 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.

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

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

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

- If you are configuring DHCP: `ifconfig e0M -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 e0M -addr=filer_addr -mask=netmask -gw=gateway`
  - `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.



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

## Boot the recovery image - FAS70 and FAS90

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

### Steps

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

The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the var file system:

If your system is running...	Then...
ONTAP 9.16.0 or earlier	<p>a. On the impaired controller, press <b>Y</b> when you see <code>Do you want to restore the backup configuration now?</code></p> <p>b. On the impaired controller, press <b>Y</b> when prompted to overwrite <code>/etc/ssh/ssh_host_ecdsa_key</code>.</p> <p>c. On the healthy partner controller, set the impaired controller to advanced privilege level: <i>set -privilege advanced</i>.</p> <p>d. On the healthy partner controller, run the restore backup command: <code>system node restore-backup -node local -target-address impaired_node_IP_address</code>.</p> <p><b>NOTE:</b> If you see any message other than a successful restore, contact <a href="#">NetApp Support</a>.</p> <p>e. On the healthy partner controller, return the impaired controller to admin level: <code>set -privilege admin</code>.</p> <p>f. On the impaired controller, press <b>y</b> when you see <code>Was the restore backup procedure successful?.</code></p> <p>g. On the impaired controller, press <b>y</b> when you see <code>...would you like to use this restored copy now?.</code></p> <p>h. On the impaired controller, press <b>y</b> when prompted to reboot the impaired controller and press <code>ctrl-c</code> for the Boot Menu.</p> <p>i. If the system does not use encryption, select <i>Option 1 Normal Boot.</i>, otherwise go to <a href="#">Restore key managers</a>.</p> <p>j. Connect the console cable to the partner controller.</p> <p>k. Give back the controller using the <i>storage failover giveback -fromnode local</i> command.</p> <p>l. Restore automatic giveback if you disabled it by using the <i>storage failover modify -node local -auto-giveback true</i> command.</p> <p>m. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the <code>system node autosupport invoke -node * -type all -message MAINT=END</code> command.</p> <p><b>NOTE:</b> If the process fails, contact <a href="#">NetApp Support</a>.</p>

## Restore encryption - FAS70 and FAS90

Restore encryption on the replacement boot media.

You must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled using the settings that you captured at the beginning of the boot media replace procedure.

Depending on which a key manger is configured on your system, select one of the following options to restore it from the boot menu.

- [Option 1: Restore the Onboard Key Manager configuration](#)
- [Option 2: Restore the External Key Manager configuration](#)

## Option 1: Restore the Onboard Key Manager configuration

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

### Before you begin

- Make sure you have following information while restoring the OKM configuration:
  - Cluster-wide passphrase entered [while enabling onboard key management](#).
  - [Backup information for the Onboard Key Manager](#).
- Perform the [How to verify onboard key management backup and cluster-wide passphrase](#) procedure before proceeding.

### Steps

1. Connect the console cable to the target controller.
2. From the ONTAP boot menu select the appropriate option from the boot menu.

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; margin: 10px 0;"> <pre> Please choose one of the following:  (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)? 10           </pre> </div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p data-bbox="621 163 1365 195">Select the hidden option <code>recover_onboard_keymanager</code></p> <p data-bbox="621 233 948 264"><b>Show example boot menu</b></p> <div data-bbox="654 306 1455 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p data-bbox="683 342 1292 373">Please choose one of the following:</p> <ul style="list-style-type: none"> <li data-bbox="688 422 976 453">(1) Normal Boot.</li> <li data-bbox="688 464 1133 495">(2) Boot without <code>/etc/rc</code>.</li> <li data-bbox="688 506 1045 537">(3) Change password.</li> <li data-bbox="683 548 1365 611">(4) Clean configuration and initialize all disks.</li> <li data-bbox="688 621 1154 653">(5) Maintenance mode boot.</li> <li data-bbox="688 663 1328 695">(6) Update flash from backup config.</li> <li data-bbox="688 705 1240 737">(7) Install new software first.</li> <li data-bbox="688 747 976 779">(8) Reboot node.</li> <li data-bbox="688 789 1192 852">(9) Configure Advanced Drive Partitioning.</li> </ul> <p data-bbox="683 863 980 894">Selection (1-19)?</p> <p data-bbox="683 905 1138 936"><code>recover_onboard_keymanager</code></p> </div>

3. Confirm that you want to continue the recovery process.

**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 will 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.

Show example prompt

Enter the backup data:

```
-----BEGIN BACKUP-----
01234567890123456789012345678901234567890123456789012345678901234567890123
12345678901234567890123456789012345678901234567890123456789012345678901234
23456789012345678901234567890123456789012345678901234567890123456789012345
34567890123456789012345678901234567890123456789012345678901234567890123456
45678901234567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
01234567890123456789012345678901234567890123456789012345678901234567890123
12345678901234567890123456789012345678901234567890123456789012345678901234
23456789012345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----
```

b. Press the enter key twice at the end of the input.

The recovery process completes.



### 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)
```

8. From the partner node, giveback the partner controller by entering the following command.

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

9. After booting with only the CFO aggregate, run the following command.

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

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

## 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. Ensure that all keys are synced by entering the following command.

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

```
There are no entries matching your query.
```



No results should appear when filtering for false in the restored parameter.

12. Giveback the node from the partner by entering the following command.

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

13. Restore automatic giveback, if you disabled it, by entering the following command.

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

14. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

## Option 2: Restore the External Key Manager configuration

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

### Before you begin

You need the following information for restoring the External Key Manager (EKM) configuration.

- A copy of the `/cfcard/kmip/servers.cfg` file from another cluster node or the following information:
  - The KMIP server address.
  - The KMIP port.
- A copy of the `/cfcard/kmip/certs/client.crt` file from another cluster node or the client certificate.

- A copy of the `/cfcard/kmip/certs/client.key` file from another cluster node or the client key.
- A copy of the `/cfcard/kmip/certs/CA.pem` file from another cluster node or the KMIP server CA(s).

## Steps

1. Connect the console cable to the target 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. When prompted, confirm you have gathered the required information.

### 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. When prompted, enter the client and server information.

### Show prompt

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

## Show example

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQLIEwpcDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUubQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpzbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----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-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----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
```

After you enter the client and server information, the recovery process completes.

## Show example

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: 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, by entering the following command.

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

7. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

## Return the failed part to NetApp - FAS70 and FAS90

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 © 2024 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.