



## **Boot media - manual recovery**

Install and maintain

NetApp  
February 13, 2026

# Table of Contents

Boot media - manual recovery .....	1
Boot media manual recovery workflow - AFF A70 and AFF A90 .....	1
Requirements for manual boot media recovery - AFF A70 and AFF A90 .....	2
Check encryption support for manual boot media recovery - AFF A70 and AFF A90 .....	2
Step 1: Check NVE support and download the correct ONTAP image .....	2
Step 2: Verify key manager status and back up configuration .....	3
Shut down the controller for manual boot media recovery - AFF A70 and AFF A90 .....	6
Replace the boot media and prepare for manual boot recovery - AFF A70 and AFF A90 .....	9
Step 1: Replace the boot media .....	9
Step 2: Transfer the boot image to the boot media .....	10
Manual boot media recovery from a USB drive - AFF A70 and AFF A90 .....	11
Restore encryption keys after manual boot recovery - AFF A70 and AFF A90 .....	14
Return the failed part to NetApp - AFF A70 and AFF A90 .....	24

# Boot media - manual recovery

## Boot media manual recovery workflow - AFF A70 and AFF A90

The manual recovery of the boot image involves using a USB drive to reinstall ONTAP onto the AFF A70 or AFF A90 system's replacement boot media. You must download the appropriate ONTAP recovery image from the NetApp Support Site and copy it to a USB drive. This prepared USB drive is then used to perform the recovery and restore the system to operational status.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, use the manual boot recovery procedure.

To get started, review the recovery requirements, shut down the controller, replace the boot media, use the USB drive to restore the image, and reapply encryption settings if necessary.

1

### [Review requirements to replace the boot media](#)

Review the requirements for replacing the boot media.

2

### [Check encryption key support and status](#)

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

3

### [Shut down the controller](#)

Shut down the controller when you need to replace the boot media.

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.

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 ONTAP 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.

# Requirements for manual boot media recovery - AFF A70 and AFF A90

Before replacing the boot media in your AFF A70 or AFF A90 system, ensure you meet the necessary requirements for a successful replacement. This includes making sure you have a USB flash drive with the appropriate amount of storage and verifying that you have the correct replacement boot device.

If your system is running in ONTAP 9.17.1 and later, use the [automatic boot recovery procedure](#).

## USB flash drive

- Ensure you have a USB flash drive formatted to FAT32.
- The USB must have sufficient storage capacity to hold the `image_xxx.tgz` file.

## File preparation

Copy the `image_xxx.tgz` file to the USB flash drive. This file will be used when you transfer the ONTAP image using the USB flash drive.

## Component replacement

Replace the failed component with the replacement component provided by NetApp.

## Controller identification

It is critical to apply the commands to the correct controller when you are replacing the impaired boot media:

- The *impaired controller* is the controller on which you are performing maintenance.
- The *healthy controller* is the HA partner of the impaired controller.

## What's next?

After you've reviewed the requirements to replace the boot media, you need to [check encryption key support and status on the boot media](#).

# Check encryption support for manual boot media recovery - AFF A70 and AFF A90

To ensure data security on your AFF A70 or AFF A90 storage system, you need to verify the encryption key support and status on your boot media. Check if your ONTAP version supports NetApp Volume Encryption (NVE), and before you shut down the controller check if the key manager is active.

If your system is running in ONTAP 9.17.1 and later, use the [automatic boot recovery procedure](#).

## 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 10No-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, EKM is listed in the command output.</li><li>• If OKM is enabled, OKM is listed in the command output.</li><li>• If no key manager is enabled, No key manager keystores configured 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, external is listed in the command output.</li><li>• If OKM is enabled, onboard is listed in the command output.</li><li>• If no key manager is enabled, No key managers configured 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:**

- 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.

- Verify that all authentication keys are restored:

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

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

- 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:**

- Back up the OKM information:

- Switch to advanced privilege mode:

```
set -priv advanced
```

Enter y when prompted to continue.

- Display the key management backup information:

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

- 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.

- Return to admin mode:

```
set -priv admin
```

- 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.

- ol style="list-style-type: none;">- 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.

- ol style="list-style-type: none;">- c. Back up the OKM information:

- ol style="list-style-type: none;">- i. Switch to advanced privilege mode:

```
set -priv advanced
```

Enter y when prompted to continue.

- ol style="list-style-type: none;">- ii. Display the key management backup information:

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

- ol style="list-style-type: none;">- 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.

- ol style="list-style-type: none;">- iv. Return to admin mode:

```
set -priv admin
```

- ol style="list-style-type: none;">- d. You can safely shut down the impaired controller and proceed to the shutdown procedure.

#### What's next?

After checking the encryption key support and status on the boot media, you need to [shut down the controller](#).

## Shut down the controller for manual boot media recovery - AFF A70 and AFF A90

Shut down the impaired controller in your AFF A70 or AFF A90 storage system to prevent data loss and maintain system stability during the automated boot media recovery process.

## 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:

- a. Enter the following command from the console of the healthy controller:

```
storage failover modify -node impaired_node_name -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 <i>y</i> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

### 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:

- a. Enter the following command from the console of the healthy controller:

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

- b. Enter *y* when you see the prompt *Do you want to disable auto-giveback?*

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 <i>y</i> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt (enter system password)	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode <i>impaired_node_name</i> -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

### What's next?

After shutting down the controller, you need to [replace the boot media](#).

## Replace the boot media and prepare for manual boot recovery - AFF A70 and AFF A90

The boot media in your AFF A70 or AFF A90 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, and then manually transferring the ONTAP image to the replacement boot media using a USB flash drive.

### 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.

#### Steps

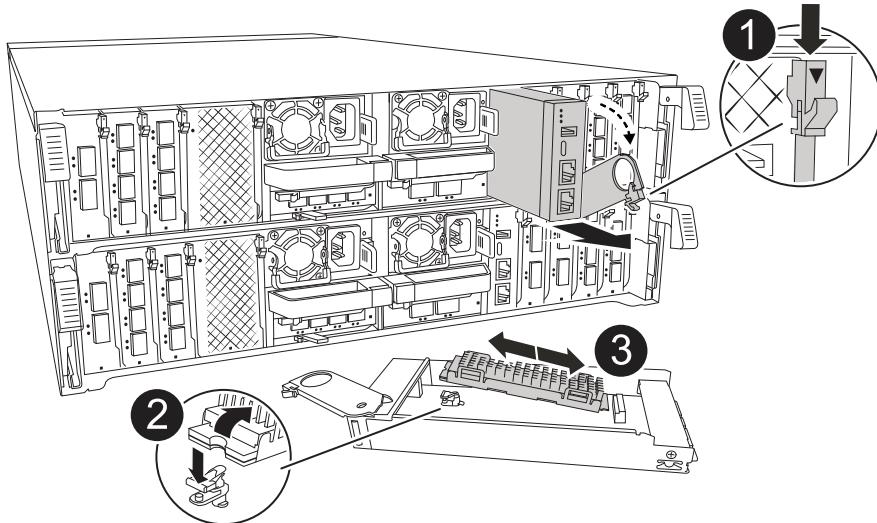
1. Go to the rear of the chassis. If you are not already grounded, properly ground yourself.
2. Unplug the controller's PSUs.



If your system has DC power, disconnect the power block from the PSUs.

- a. Remove any cables connected to the System Management module. Make sure to 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. The cam lever moves away from the chassis.
- d. Rotate the cam lever all the way down and remove the System Management module from the controller module.
- e. 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:



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

- 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. Rotate the cable management tray up to the closed position.
  - b. Recable the System Management module.

## Step 2: Transfer the boot 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 a 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-A port 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 cords into the power supplies. The controller reboots as soon as power is restored.



If you have DC power supplies, reconnect the power block to the power supplies.

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.

## What's next?

After replacing the boot media, you need to [boot the recovery image](#).

## Manual boot media recovery from a USB drive - AFF A70 and AFF A90

After installing the new boot media device in your AFF A70 or AFF A90 system, you can boot the recovery image manually from a USB drive to restore the configuration from the partner node.

If your system is running in ONTAP 9.17.1 and later, use the [automatic boot recovery procedure](#).

### Before you begin

- Ensure your console is connected to the impaired controller.
- Verify you have a USB flash drive with the recovery image.

- Determine if your system uses encryption. You will need to select the appropriate option in step 3 based on whether encryption is enabled.

## Steps

1. From the LOADER prompt on the impaired controller, boot the recovery image from the USB flash drive:

```
boot_recovery
```

The recovery image is downloaded from the USB flash drive.

2. When prompted, enter the name of the image or press **Enter** to accept the default image displayed in brackets.

3. Restore the var file system using the procedure for your ONTAP version:

## ONTAP 9.16.0 or earlier

Complete the following steps on the impaired controller and partner controller:

- a. **On the impaired controller:** Press Y when you see Do you want to restore the backup configuration now?
- b. **On the impaired controller:** If prompted, press Y to overwrite `/etc/ssh/ssh_host_ecdsa_key`.
- c. **On the partner controller:** Set the impaired controller to advanced privilege level:

```
set -privilege advanced
```

- d. **On the partner controller:** Run the restore backup command:

```
system node restore-backup -node local -target-address  
impaired_node_IP_address
```



If you see any message other than a successful restore, contact NetApp Support.

- e. **On the partner controller:** Return to admin level:

```
set -privilege admin
```

- f. **On the impaired controller:** Press Y when you see Was the restore backup procedure successful?
- g. **On the impaired controller:** Press Y when you see ...would you like to use this restored copy now?
- h. **On the impaired controller:** Press Y when prompted to reboot, then press `Ctrl-C` when you see the Boot Menu.
- i. **On the impaired controller:** Do one of the following:
  - If the system does not use encryption, select *Option 1 Normal Boot* from the Boot Menu.
  - If the system uses encryption, go to [Restore encryption](#).

## ONTAP 9.16.1 or later

Complete the following steps on the impaired controller:

- a. Press Y when prompted to restore the backup configuration.

After the restore procedure is successful, this message displays: `syncflash_partner:`  
`Restore from partner complete`

- b. Press Y when prompted to confirm that the restore backup was successful.
- c. Press Y when prompted to use the restored configuration.
- d. Press Y when prompted to reboot the node.
- e. Press Y when prompted to reboot again, then press `Ctrl-C` when you see the Boot Menu.
- f. Do one of the following:
  - If the system does not use encryption, select *Option 1 Normal Boot* from the Boot Menu.

- If the system uses encryption, go to [Restore encryption](#).

4. Connect the console cable to the partner controller.
5. Return the controller to normal operation by giving back its storage:

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

6. If you disabled automatic giveback, reenable 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
```

#### What's next?

After booting the recovery image, you need to [restore encryption on the boot media](#).

## Restore encryption keys after manual boot recovery - AFF A70 and AFF A90

Restore encryption on the replacement boot media in your AFF A70 or AFF A90 system to ensure continued data protection. The replacement process involves verifying key availability, reapplying encryption settings, and confirming secure access to your data.

If your system is running in ONTAP 9.17.1 and later, use the [automatic boot recovery procedure](#).

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; width: fit-content; margin: 10px auto; border-radius: 10px;"><p>Please choose one of the following:</p><p>(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</p></div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p>Select the hidden option <code>recover_onboard_keymanager</code></p> <p><b>Show example boot menu</b></p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; background-color: #f9f9f9;"> <p style="margin: 0;">Please choose one of the following:</p> <p style="margin: 0;">(1) Normal Boot.</p> <p style="margin: 0;">(2) Boot without /etc/rc.</p> <p style="margin: 0;">(3) Change password.</p> <p style="margin: 0;">(4) Clean configuration and initialize all disks.</p> <p style="margin: 0;">(5) Maintenance mode boot.</p> <p style="margin: 0;">(6) Update flash from backup config.</p> <p style="margin: 0;">(7) Install new software first.</p> <p style="margin: 0;">(8) Reboot node.</p> <p style="margin: 0;">(9) Configure Advanced Drive Partitioning.</p> <p style="margin: 0;">Selection (1-19)?</p> <p style="margin: 0;">recover_onboard_keymanager</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.

## Show example prompt

Enter the backup data:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
0123456789012345678901234567890123456789012345678901  
23  
1234567890123456789012345678901234567890123456789012  
34  
2345678901234567890123456789012345678901234567890123  
45  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAA  
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/kmip/servers.cfg file or the KMIP server address and port
- /cfcard/kmip/certs/client.crt file (client certificate)
- /cfcard/kmip/certs/client.key file (client key)
- /cfcard/kmip/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
```

### What's next?

After restoring encryption on the boot media, you need to [return the failed part to NetApp](#).

## Return the failed part to NetApp - AFF A70 and AFF A90

If a component in your AFF A70 or AFF A90 storage system fails, return the failed part to NetApp. 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.