



# Boot media

## Install and maintain

NetApp  
July 19, 2024

# Table of Contents

- Boot media ..... 1
  - Overview of boot media replacement - FAS2800 ..... 1
  - Check onboard encryption keys - FAS2800 ..... 1
  - Shut down the impaired controller - FAS2800 ..... 5
  - Replace the boot media - FAS2800 ..... 5
  - Boot the recovery image - FAS2800 ..... 9
  - Restore OKM, NSE, and NVE as needed - FAS2800 ..... 11
  - Return the failed part to NetApp - FAS2800 ..... 13

# Boot media

## Overview of boot media replacement - FAS2800

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_XXX.tgz` file.

You also must copy the `image_XXX.tgz` file to the USB flash drive for later use in this procedure.

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

## Check onboard encryption keys - FAS2800

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy 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. Check the status of the impaired controller:
  - If the impaired controller is at the login prompt, log in as `admin`.
  - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

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

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

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

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
  - If `<Ino-DARE>` or `<1Ono-DARE>` is displayed in the command output, the system does not support NVE, proceed to [Shut down the impaired controller](#).
  - If `<Ino-DARE>` is not not displayed in the command output, and the system is running ONTAP 9.6 or later, continue to the next section, [Check NVE or NSE on systems running ONTAP 9.6 and later](#).
4. Disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false`` or `storage failover modify -node local -auto-giveback-after-panic false`

## Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
  - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
  - If no disks are shown, NSE is not configured.
  - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

## Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key query`



After the ONTAP 9.6 release, you may have additional key manager types. The types are KMIP, AKV, and GCP. The process for confirming these types is the same as confirming external or onboard key manager types.

- If the Key Manager type displays `external` and the Restored column displays `yes`, it's safe to shut down the impaired controller.
  - If the Key Manager type displays `onboard` and the Restored column displays `yes`, you need to complete some additional steps.
  - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
  - If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
2. If the Key Manager type displays `onboard` and the Restored column displays `yes`, manually back up the OKM information:
    - a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- b. Enter the command to display the key management information: `security key-manager onboard show-backup`
  - c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
  - d. Return to admin mode: `set -priv admin`
  - e. Shut down the impaired controller.
3. If the Key Manager type displays `external` and the Restored column displays anything other than `yes`:
- a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`
- If the command fails, contact NetApp Support.
- [mysupport.netapp.com](https://mysupport.netapp.com)
- b. Verify that the Restored column equals `yes` for all authentication keys: `security key-manager key query`
  - c. Shut down the impaired controller.
4. If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`:
- a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`



Enter the customer's 32 character, alphanumeric onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.  
[mysupport.netapp.com](https://mysupport.netapp.com)

- b. Verify the Restored column shows `yes` for all authentication keys: `security key-manager key query`
- c. Verify that the Key Manager type shows `onboard`, and then manually back up the OKM information.
- d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
- f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- g. Return to admin mode: `set -priv admin`
- h. You can safely shut down the controller.

## Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key query -key-type NSE-AK`



After the ONTAP 9.6 release, you may have additional key manager types. The types are KMIP, AKV, and GCP. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the Key Manager type displays `external` and the Restored column displays `yes`, it's safe to shut down the impaired controller.
  - If the Key Manager type displays `onboard` and the Restored column displays `yes`, you need to complete some additional steps.
  - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
  - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
2. If the Key Manager type displays `onboard` and the Restored column displays `yes`, manually back up the OKM information:
    - a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
    - b. Enter the command to display the key management information: `security key-manager onboard show-backup`
    - c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
    - d. Return to admin mode: `set -priv admin`
    - e. You can safely shut down the controller.
  3. If the Key Manager type displays `external` and the Restored column displays anything other than `yes`:
    - a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`  
  
If the command fails, contact NetApp Support.  
  
[mysupport.netapp.com](https://mysupport.netapp.com)
    - b. Verify that the Restored column equals `yes` for all authentication keys: `security key-manager key query`
    - c. You can safely shut down the controller.
  4. If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`:
    - a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`  
  
Enter the customer's 32 character, alphanumeric onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.  
  
[mysupport.netapp.com](https://mysupport.netapp.com)
    - b. Verify the Restored column shows `yes` for all authentication keys: `security key-manager key query`
    - c. Verify that the Key Manager type shows `onboard`, and then manually back up the OKM information.
    - d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
    - e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

- f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- g. Return to admin mode: `set -priv admin`
- h. You can safely shut down the controller.

## Shut down the impaired controller - FAS2800

Shut down or take over the impaired controller.

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.

## Replace the boot media - FAS2800

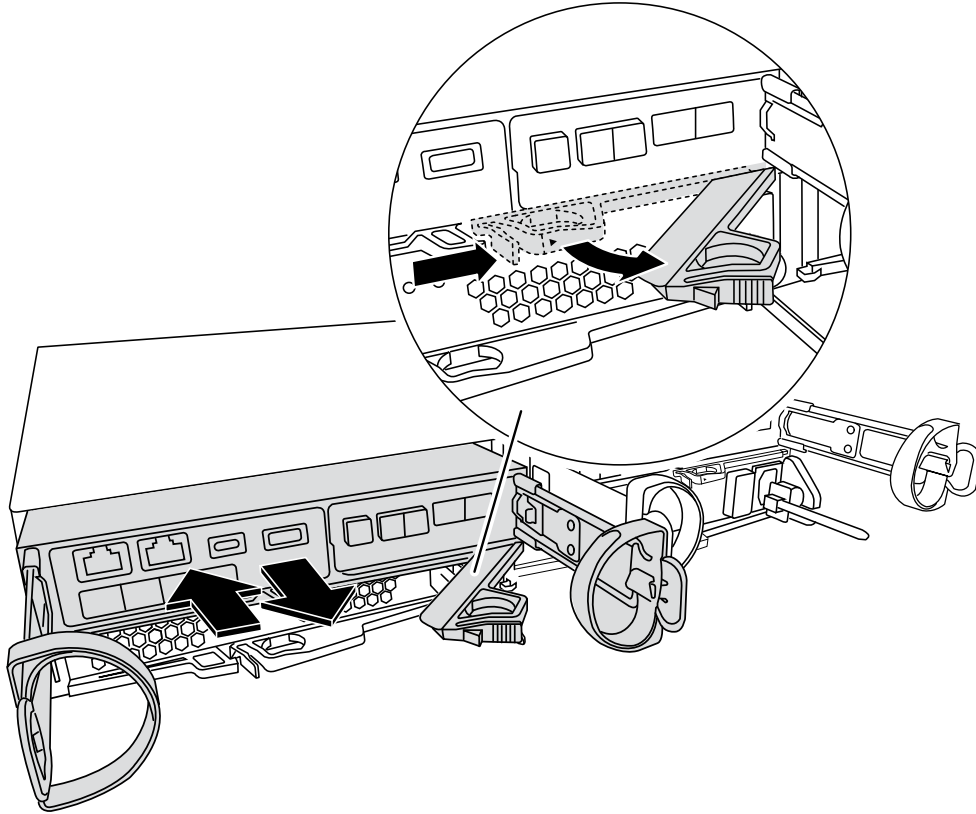
To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

### Step 1: Remove the controller module

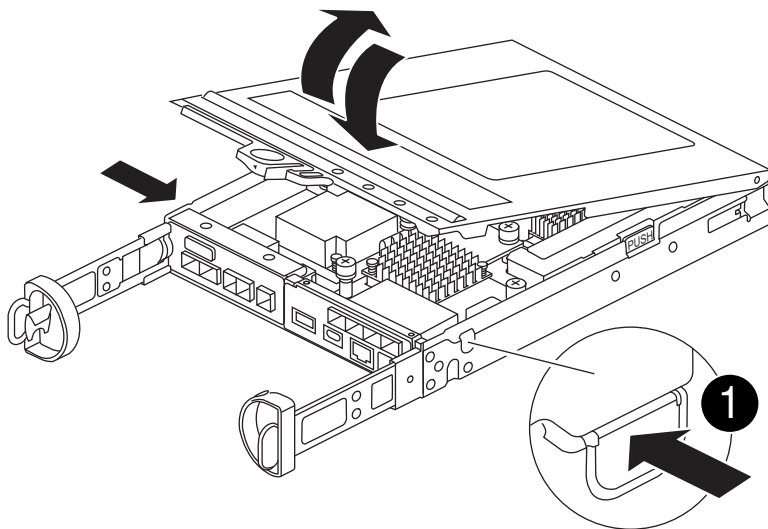
To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

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.

3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



4. Turn the controller module over and place it on a flat, stable surface.
5. Open the cover by pressing the blue buttons on the sides of the controller module to release the cover, and then rotate the cover up and off of the controller module.



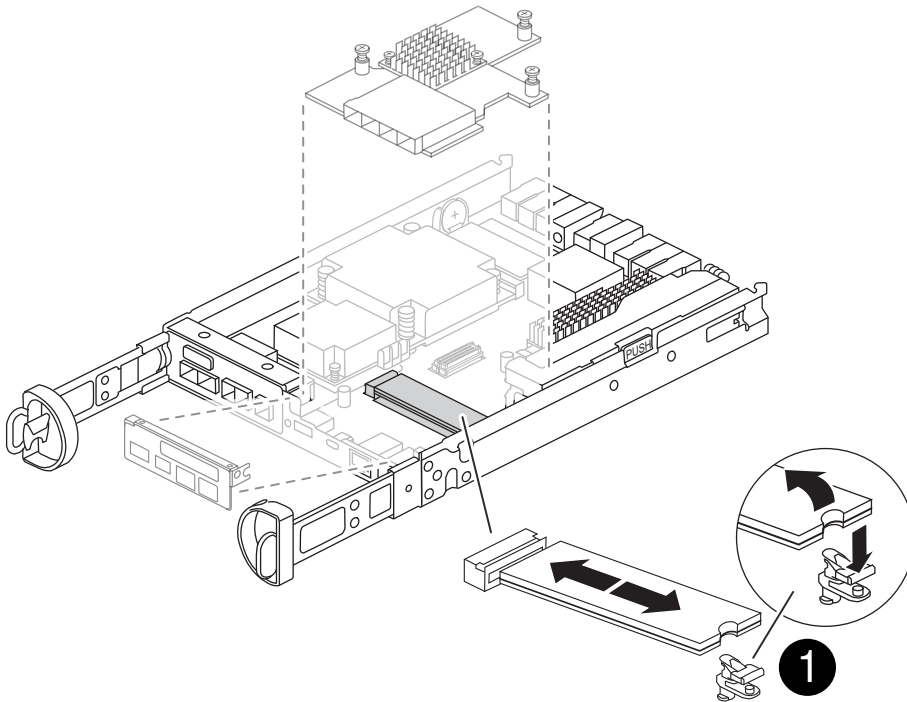
<b>1</b>	Controller module cover release button
----------	----------------------------------------



## Step 2: Replace the boot media

Locate the boot media in the controller module, located under the mezzanine card and follow the directions to replace it.

[Animation - Replace the boot media](#)



<b>1</b>	Boot media locking tab
----------	------------------------

### Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the mezzanine card using the following illustration or the FRU map on the controller module:
  - a. Remove the IO Plate by sliding it straight out from the controller module.
  - b. Loosen the thumbscrews on the mezzanine card.



You can loosen the thumbscrews with your fingers or a screwdriver. If you use your fingers, you might need to rotate the NV battery up for better finger purchase on the thumbscrew next to it.

- c. Lift the mezzanine card straight up.
3. Replace the boot media:
    - a. Press the blue button on the boot media housing to release the boot media from its housing, rotate the boot media up, 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.

- b. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket. Check the boot media to make sure that it is seated squarely and completely in the socket, and if necessary, remove the boot media and reseat it into the socket.
  - c. Push the blue locking button, rotate the boot media all the way down, and then release the locking button to lock the boot media in place.
4. Reinstall the mezzanine card:
  - a. Align the socket on the motherboard with the socket on the mezzanine card, and then gently seat the card in the socket.
  - b. Tighten the three thumbscrews on the mezzanine card.
  - c. Reinstall the IO Plate.
5. Reinstall the controller module cover and lock it into place.

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

Install the system image on the replacement boot media using a USB flash drive with the image installed on it. You must restore the var file system during this procedure.

#### Before you begin

- You must have a USB flash drive, formatted to MBR/FAT32, with at least 4GB capacity.
- You must have a network connection.

#### Steps

1. Download the appropriate image version of ONTAP to the formatted USB flash drive:
  - a. Use [How to determine if the running ONTAP version supports NetApp Volume Encryption \(NVE\)](#) to determine if volume encryption is currently supported.
    - If NVE is supported on the cluster, download the image with NetApp Volume Encryption.
    - If NVE is not supported on the cluster, download the image without NetApp Volume Encryption. See [Which ONTAP image should I download? With or without Volume Encryption?](#) for more details.
2. Unzip the downloaded image.



If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

There are two folders in the unzipped service image file:

- boot
- efi

- a. Copy the efi folder to the top directory on the USB flash drive.

The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

- b. Remove the USB flash drive from your laptop.

3. Install the controller module:

- a. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

- b. Recable the controller module.

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

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

## Boot the recovery image - FAS2800

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

4. Ensure that the environmental variables are set as expected:
  - a. Take the controller to the LOADER prompt.
  - b. Check the environment variable settings with the `printenv` command.
  - c. If an environment variable is not set as expected, modify it with the `setenv environment-variable-name changed-value` command.
  - d. Save your changes using the `savenv` command.
5. The next depends on your system configuration:
  - If your system has onboard keymanager, NSE or NVE configured, go to [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.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see...	Then...
The login prompt	Go to the next Step.
Waiting for giveback...	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the <code>storage failover show</code> command.

7. 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 show -is-home false` command.

If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert -vserver vservice_name -lif lif_name` command.

10. Move the console cable to the repaired controller and run the `version -v` command to check the ONTAP versions.

11. If you are not using storage encryption, restore automatic giveback and AutoSupport:

a. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

b. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

## Restore OKM, NSE, and NVE as needed - FAS2800

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled using settings you captured at the beginning of this procedure.



If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

### Steps

1. Connect the console cable to the target controller.

2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.

3. Check the console output:

If the console displays...	Then...
The login prompt	Go to Step 7.

If the console displays...	Then...
Waiting for giveback...	<ol style="list-style-type: none"> <li>a. Log into the partner controller.</li> <li>b. Confirm the target controller is ready for giveback with the <code>storage failover show</code> command.</li> </ol>

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
  - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
  - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.



Terminating CIFS can cause loss of data.

- If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
  - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
  6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert -vserver Cluster -lif nodename` command.

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
  - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
  - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.



If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

Use the security key-manager key query to verify that the Restored column = yes/true for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
14. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the `system node autosupport invoke -node * -type all -message MAINT=END`

## Return the failed part to NetApp - FAS2800

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