Boot media

Install and maintain

NetApp
February 28, 2025

Table of Contents

Boot media

Overview of boot media recovery - AFF A20, AFF A30, and AFF A50

Boot media recovery uses the boot image from the partner node and automatically runs the appropriate boot menu option to install the boot image on the replacement boot media.

When you encounter boot error messages similar to the one shown below, you need to replace the boot media and restore the ONTAP image from the partner node.

```
Can't find primary boot device u0a.0
Can't find backup boot device u0a.1
ACPI RSDP Found at 0x777fe014

Starting AUTOBOOT press Ctrl-C to abort...
Could not load fat://boot0/X86_64/freebsd/image1/kernel: Device not found

ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/Linux/image1/vmlinuz (boot0, fat)
ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/freebsd/image1/kernel (boot0, fat)

Autoboot of PRIMARY image failed. Device not found (-6)
LOADER-A>
```

Boot media replacement workflow - AFF A20, AFF A30, and AFF A50

Follow these workflow steps to replace your boot media.

1 **Review the boot media requirements**

Review the requirements for boot media replacement.

2 **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.

3 **Replace the boot media**

Remove the failed boot media from the impaired controller and install the replacement boot media.

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

Restore the ONTAP image from the healthy controller.

5 **Return the failed part to NetApp**

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

Requirements - AFF A20, AFF A30, and AFF A50

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

Requirements

- You must replace the failed component with a replacement FRU component of the same capacity that you received from NetApp.
- The e0S (e0M wrench) port on the impaired controller cannot be faulty.

  The e0S port is used for automated boot recovery.

- Determine if Onboard Key Manger (OKM) or Eternal Key Manager (EKM) is configured using one of the following methods:
  - You can ask the system administrator if OKM or EKM are enabled.
  - To check if OKM is enabled, you can use the `security key-manager onboard show`.
  - To check if EKM is enabled, you can use the `security key-manager external show`.
- For OKM, you need the OKM passphrase file contents.
- For EKM, you need copies of the following files from the partner node:
  - /cfcard/kmip/servers.cfg file.
  - /cfcard/kmip/certs/client.crt file.
  - /cfcard/kmip/certs/client.key file.
  - /cfcard/kmip/certs/CA.pem file.

Considerations

- 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.
- If needed, you can turn on the platform chassis location (blue) LEDs to aid in physically locating the affected platform. Log into the BMC using SSH and enter the `system location-led` *on* command.

  A platform chassis has three location LEDs: one on the operator display panel and one on each controller. Location LEDs remain illuminated for 30 minutes.

  You can turn them off by entering the `system location-led` *off* command. If you are unsure if the

LEDs are on or off, you can check their state by entering the `system location-led show` command.

What's next

After you've reviewed the boot media requirements, shut down the impaired controller.

Shut down the controller - AFF A20, AFF A30, and AFF A50

You need to complete the shutdown of the impaired controller. Shut down or take over the impaired controller.

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 `y` when prompted.

If the impaired controller is displaying…	Then…
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`* When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

What's next

After you shut down the impaired controller, replace the boot media.

Replace the boot media - AFF A20, AFF A30, and AFF A50

To replace the boot media, you must remove the impaired controller, remove the impaired boot media, and install the replacement boot media in the impaired controller.

Step 1: Remove the controller

You must remove the controller from the chassis when you replace the controller or replace a component inside the controller.

Before you begin

All other components in the storage system must be functioning properly; if not, you must contact NetApp Support before continuing with this procedure.

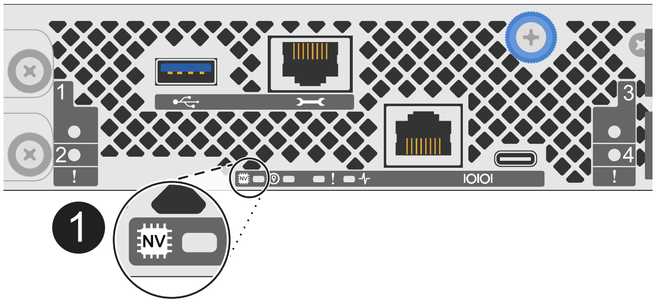
Steps

1. On the impaired controller, make sure the NV LED is off.

   When the NV LED is off, destaging is complete and it is safe to remove the impaired controller.

   > If the NV LED is flashing (green), destage is in progress. You must wait for the NV LED to turn off. However, if the flashing continues for longer than five minutes, contact NetApp Support before continuing with this procedure.

   The NV LED is located next to the NV icon on the controller.



1	NV icon and LED on the controller

2. If you are not already grounded, properly ground yourself.
3. Disconnect the power on the impaired controller:

   > ⓘ Power supplies (PSUs) do not have a power switch.

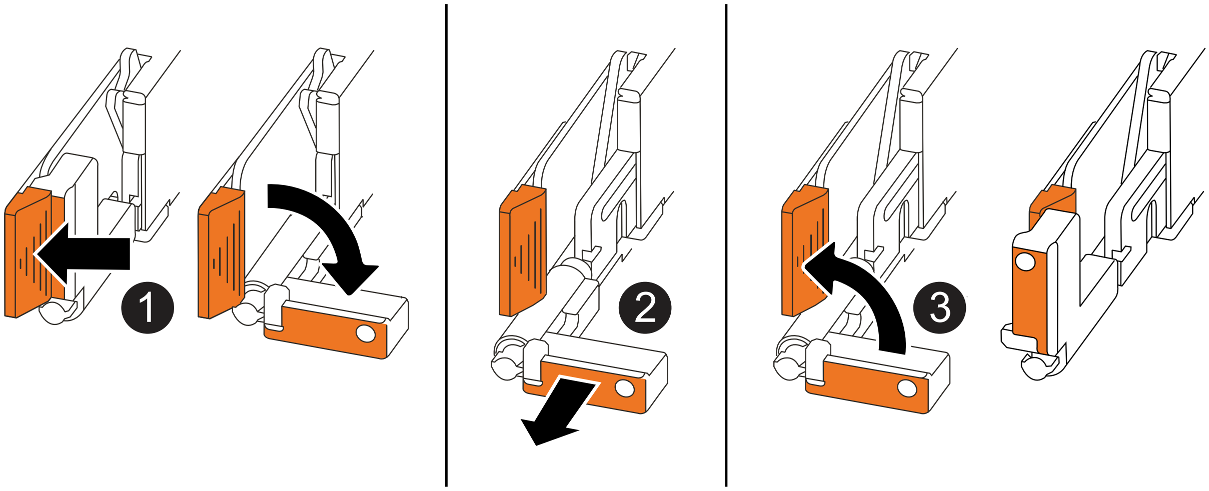
If you are disconnecting a…	Then…
AC PSU	1. Open the power cord retainer. 2. Unplug the power cord from the PSU and set it aside.
DC PSU	1. Unscrew the two thumb screws on the D-SUB DC power cord connector. 2. Unplug the power cord from the PSU and set it aside.

4. Unplug all cables from the impaired controller.

   Keep track of where the cables were connected.

5. Remove the impaired controller:

   The following illustration shows the operation of the controller handles (from the left side of the controller) when removing a controller:



1	On both ends of the controller, push the vertical locking tabs outward to release the handles.

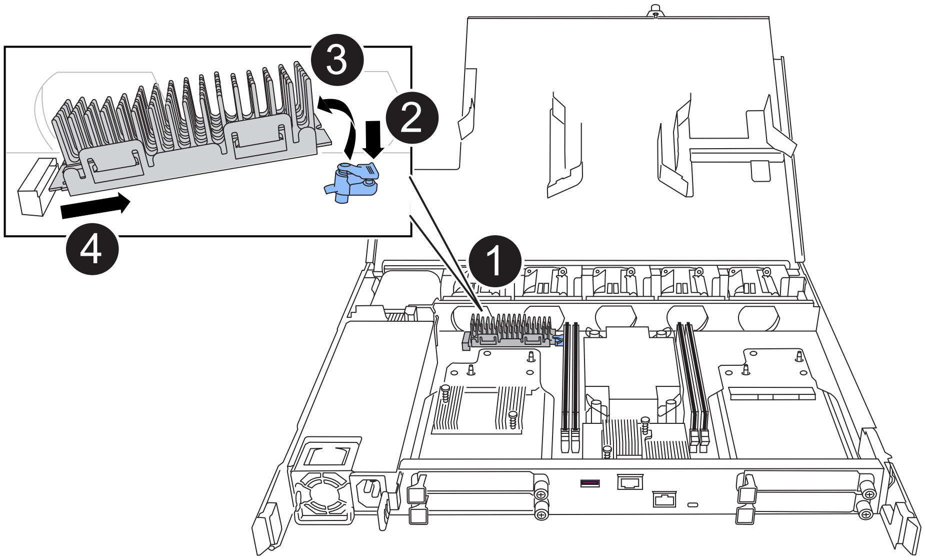
❷	• Pull the handles towards you to unseat the controller from the midplane. As you pull, the handles extend out from the controller and then you feel some resistance, keep pulling. • Slide the controller out of the chassis while supporting the bottom of the controller, and place it on a flat, stable surface.
❸	If needed, rotate the handles upright (next to the tabs) to move them out of the way.

6. Place the controller on an anti-static mat.
7. Open the controller cover by turning the thumbscrew counterclockwise to loosen, and then open the cover.

Step 2: Replace the boot media

To replace the boot media, locate it inside the controller and follow the specific sequence of steps.

1. If you are not already grounded, properly ground yourself.
2. Remove the boot media:



❶	Boot media location
❷	Press down on the blue tab to release the right end of the boot media.
❸	Lift the right end of the boot media up at a slight angle to get a good grip along the sides of the boot media.
❹	Gently pull the left end of the boot media out of its socket.

3. Install the replacement boot media:

a. Remove the boot media from its package.

b. Slide the socket end of the boot media into its socket.

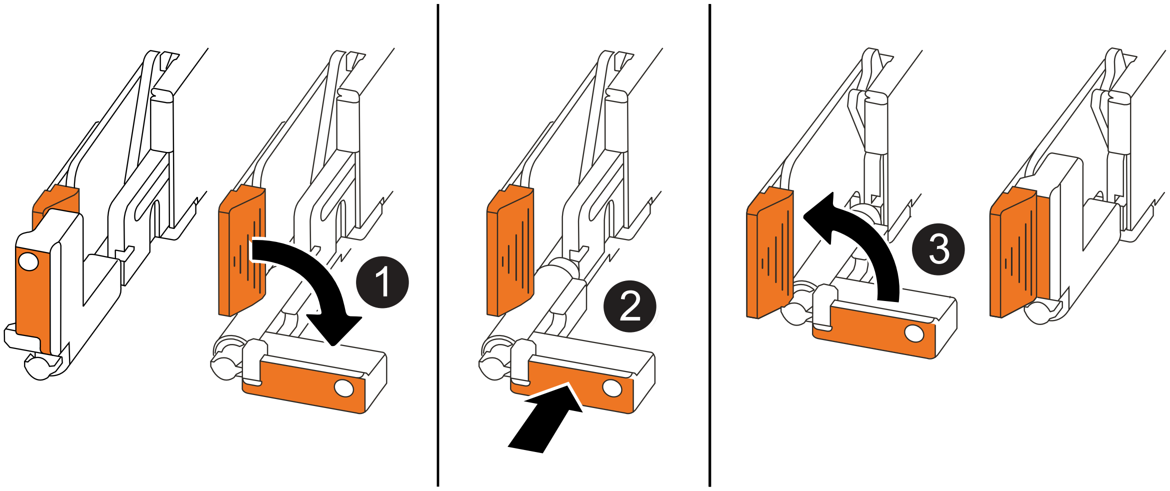
c. At the opposite end of the boot media, press down and hold the blue tab (in the open position), gently push down on that end of the boot media until it stops, and then release the tab to lock the boot media into place.

Step 3: Reinstall the controller

Reinstall the controller into the chassis and reboot it.

About this task

The following illustration shows the operation of the controller handles (from the left side of a controller) when reinstalling the controller, and can be used as a reference for the rest of the controller reinstallation steps.



❶	If you rotated the controller handles upright (next to the tabs) to move them out of the way while you serviced the controller, rotate them down to the horizontal position.
❷	Push the handles to reinsert the controller into the chassis halfway and then, when instructed, push until the controller is fully seated.
❸	Rotate the handles to the upright position and lock in place with the locking tabs.

Steps

1. Close the controller cover and turn the thumbscrew clockwise until tightened.
2. Insert the controller halfway into the chassis.

   Align the rear of the controller with the opening in the chassis, and then gently push the controller using the handles.

   > Do not completely insert the controller in the chassis until instructed to do so later in this procedure.

3. Reconnect the cables to the controller; however, do not plug in the power cord to the power supply (PSU) at this time.

ⓘ Make sure that the console cable is connected to the controller because you want to catch and log the boot sequence later in the boot media replacement procedure when you fully seat the controller in the chassis and it begins to boot.

4. Fully seat the controller in the chassis:
   a. Firmly push on the handles until the controller meets the midplane and is fully seated.

      Do not use excessive force when sliding the controller into the chassis; it could damage the connectors.

      ⓘ The controller boots when fully seated in the chassis. It gets its power from the partner controller.

   b. If the controller boots to the LOADER prompt, reboot the controller: `boot_ontap`
   c. Rotate the controller handles up and lock in place with the tabs.
5. Reconnect the power cord to the PSU on the impaired controller.

   Once power is restored to the PSU, the status LED should be green.

If you are reconnecting a…	Then…
AC PSU	1. Plug the power cord into the PSU. 2. Secure the power cord with the power cord retainer.
DC PSU	1. Plug the D-SUB DC power cord connector into the PSU. 2. Tighten the two thumb screws to secure the D-SUB DC power cord connector to the PSU.

What's next

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

Restore the ONTAP image - AFF A20, AFF A30, and AFF A50

Before you begin

- Determine if Onboard Key Manger (OKM) or Eternal Key Manager (EKM) is configured using one of the following methods:
  - You can ask the customer or system administrator if OKM or EKM are enabled.
  - To check if OKM is enabled, you can use the `security key-manager onboard show`.
  - To check if EKM is enabled, you can use the `security key-manager external show`.
- For OKM, you need the OKM passphrase file contents.
- For EKM, you need copies of the following files from the partner node:
  - /cfcard/kmip/servers.cfg file.
  - /cfcard/kmip/certs/client.crt file.

  - /cfcard/kmip/certs/client.key file.
  - /cfcard/kmip/certs/CA.pem file.

Steps

1. From the LOADER prompt, enter the command:

   `boot_recovery -partner`

   The screen displays the following message:

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

2. Monitor the boot media install recovery process.

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

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

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

   Show example of configuration error finding prompts

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

   Has key manager been configured on this system

   Is the key manager onboard
   ```

If you see this message…	Do this…
`key manager is not configured. Exiting.`	Encryption is not installed on the system. Complete the following steps: a. Log into the node when the login prompt is displayed and give back the storage: `storage failover giveback -ofnode` *`impaired_node_name`* b. Go to step 5 to enable automatic giveback if it was disabled.

If you see this message…	Do this…
`key manager is configured.`	Go to step 4 to restore the appropriate key manager. The node access the boot menu and runs: • Option 10 for systems with Onboard Key Manager (OKM). • Option 11 for systems with External Key Manager (EKM).

4. Select the appropriate key manager restoration process.

Onboard Key Manager (OKM)

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

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

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

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

b. Enter the passphrase for onboard key manager when prompted, and enter the passphrase again when prompted, to confirm.

   Show example of passphrase prompts

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

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

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

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

   Successfully recovered keymanager secrets.
   ```

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

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

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

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

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

External Key Manager (EKM)

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

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

a. The next step depends on which version of ONTAP your system is running:

If your system is running…	Do this…
ONTAP 9.16.0	a. Press `Ctlr-C` to exit BootMenu Option 11. b. Press `Ctlr-C` to exit the EKM configuration process and return to the boot menu. c. Select BootMenu Option 8. d. Reboot the node. If `AUTOBOOT` is set, the node reboots and uses the configuration files from the partner node. If `AUTOBOOT` is not set, enter the appropriate boot command. The node reboots and uses the configuration files from the partner node. e. Reboot the node so that EKM protects the boot media partition. f. Proceed to step c.
ONTAP 9.16.1	Proceed to the next step.

b. Enter the following EKM configuration setting when prompted:

Action	Example

Enter the client certificate contents from the `/cfcard/kmip/certs/client.crt` file.	**Show example of client certificate contents**
	`-----BEGIN`
	`CERTIFICATE-----`
	`<certificate_value>`
	`-----END CERTIFICATE-----`

Action	Example

Enter the client key file contents from the `/cfcard/kmip/certs/client.key` file.	**Show example of client key file contents**
	`-----BEGIN RSA PRIVATE KEY-----`
	`<key_value>`
	`-----END RSA PRIVATE KEY-----`

Enter the KMIP server CA(s) file contents from the `/cfcard/kmip/certs/CA.pem` file.	**Show example of KMIP server file contents**
	`-----BEGIN CERTIFICATE-----`
	`<KMIP_certificate_CA_value>`
	`-----END CERTIFICATE-----`

Action	Example

Enter the server configuration file contents from the `/cfcard/kmip/servers.cfg` file.	**Show example of server configuration file contents**
	`xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx`
	`xxx.xxx.xxx.xxx:5696.port=5696`
	`xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem`
	`xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4`
	`1xxx.xxx.xxx.xxx:5696.timeout=25`
	`xxx.xxx.xxx.xxx:5696.nbio=1`
	`xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.crt`
	`xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key`
	`xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL"`
	`xxx.xxx.xxx.xxx:5696.verify=true`
	`xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>`

<table>
<tr><th>Action</th><th>Example</th></tr>
<tr><td>If prompted, enter the ONTAP Cluster UUID from the partner.</td><td>

Show example of ONTAP Cluster UUID

```
Notice:
bootarg.mgwd.cluster_uuid
is not set or is empty.
Do you know the ONTAP
Cluster UUID? {y/n} y
Enter the ONTAP Cluster
UUID: <cluster_uuid_value>


System is ready to utilize
external key manager(s).
```

</td></tr>
<tr><td>If prompted, enter the temporary network interface and settings for the node.</td><td>

Show example of a temporary network setting

```
In order to recover key
information, a temporary
network interface needs to
be
configured.

Select the network port
you want to use (for
example, 'e0a')
e0M

Enter the IP address for
port : xxx.xxx.xxx.xxx
Enter the netmask for port
: xxx.xxx.xxx.xxx
Enter IP address of
default gateway:
xxx.xxx.xxx.xxx
Trying to recover keys
from key servers....
[discover_versions]
[status=SUCCESS reason=
message=]
```

</td></tr>
</table>

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

- If the EKM configuration has been successfully restored, the process attempts to restore the appropriate files from the partner node and reboots the node. Go to step d.

Show example of successful 9.16.0 restore messages

```
kmip2_client: Importing keys from external key server:
xxx.xxx.xxx.xxx:5696
[Feb  6 04:57:43]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdUtils:
[locateMrootAkUuids]:420: Locating local cluster MROOT-AK
with keystore UUID: <uuid>
[Feb  6 04:57:43]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [doCmdImp]:79: Calling
KMIP Locate for the following attributes: [<x-NETAPP-
ClusterId, <uuid>>, <x-NETAPP-KeyUsage, MROOT-AK>, <x-
NETAPP-KeystoreUuid, <uuid>>, <x-NETAPP-Product, Data
ONTAP>]
[Feb  6 04:57:44]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [doCmdImp]:84: KMIP
Locate executed successfully!
[Feb  6 04:57:44]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [setUuidList]:50: UUID
returned: <uuid>
...
kmip2_client: Successfully imported the keys from external
key server: xxx.xxx.xxx.xxx:5696

GEOM_ELI: Device nvd0s4.eli created.
GEOM_ELI: Encryption: AES-XTS 256
GEOM_ELI:     Crypto: software
Feb 06 05:02:37 [_server-name_]: crypto_get_mroot_ak:140
MROOT-AK is requested.
Feb 06 05:02:37 [_server-name_]: crypto_get_mroot_ak:162
Returning MROOT-AK.
```

Show example of successful 9.16.1 restore messages

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
...
kmip2_client: Successfully imported the keys from external
key server: xxx.xxx.xxx.xxx:xxxx
Successfully recovered keymanager secrets.
```

- If the key is not successfully restored, the system will halt and indicate that it could not restore the key. The error and warning messages are displayed. Rerun the recovery process by entering `boot_recovery -partner`.

Show example of key recovery error and warning messages

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

Uptime: 11m32s
System halting...

LOADER-B>
```

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

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

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

5. If automatic giveback was disabled, reenable it:

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

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

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

Return the failed part to NetApp - AFF A20, AFF A30, and AFF A50

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

Trademark information