Boot media

Install and maintain

NetApp
September 25, 2024

Table of Contents

Boot media

Overview of replacing the boot media - ASA A1K

You can replace a failed boot media manually by using USB module for the boot image or through the automated boot media replace (BMR) option.

- Automated boot media replacement

  Automated boot media replace uses the boot image from the partned node and automatically runs the appropriate boot menu option to install the boot image to the replacement boot media.

- Manual boot media replace

  Manual boot media replace uses the traditional method of downloading the ONTAP image from the NetApp support site, transferring the image to a USB drive, downloading it to the target replacement boot media, and manually walking through the boot menu options to install the ONTAP image on the replacement boot media.

Automated method

Boot media replacement workflow - ASA A1K

Follow these workflow steps to replace your boot media.

Review the boot media requirements

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

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.

Replace the boot media

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

Automated boot recovery

Restore the ONTAP image from the partner controller.

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 - ASA A1K

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

- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.
- There must be no faulty cluster ports on the impaired controller.

Shut down the impaired controller - ASA A1K

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:

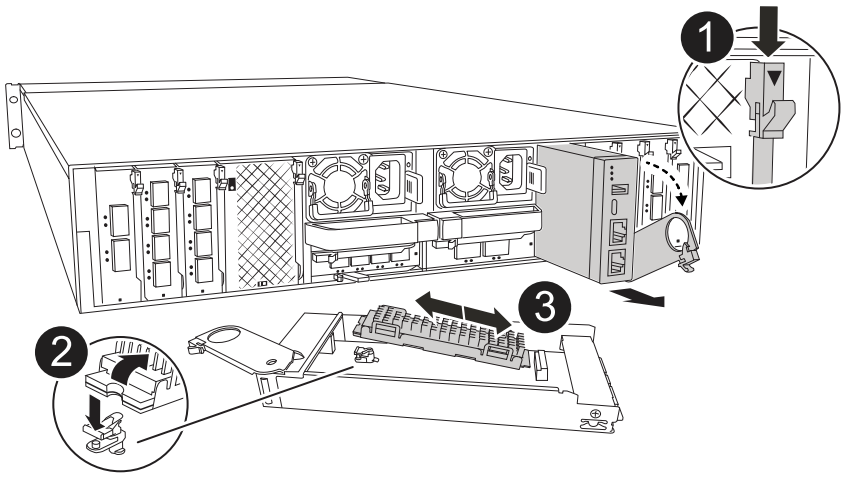
If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - ASA A1K

To replace the boot media, you must remove the System Management module from the back of the system, remove the impaired boot media, install the replacement boot media in the System Management module.

Steps

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.

Automated boot recovery - ASA A1K

You can restore image on the boot media from the partner controller using the automated boot recovery process.

Select the single node automated recovery option that matches your configuration.

Option 1: Recovery with no encryption

You can restore the ONTAP image (boot media recovery) from the partner node using the `boot_recovery -partner` command with ASA r2 platforms running ONTAP 9.16.0 and later.

Before you begin

When you boot a node and the boot media on that node is corrupted, you'll see the following messages and the boot process with stop at the LOADER prompt:

```
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>
```

If you see this message, you must restore the ONTAP image

Steps

1. From the LOADER prompt, enter the *boot_recovery -partner* command.

   The screen will displays the message `Starting boot media recovery (BMR) process press Ctrl-C to abort…` and begins initial checks.

2. Monitor the process as LOADER configures the local cluster ports and executes netboot through `http://<remote-partner-IP>:65530/recoverydisk/image.tgz`.

   Once netboot is running, `Starting BMR …` is displayed on the screen and the process completes the installation process.

   a. If Key Manager is not configured, you will see the following message:

      ```
      key manager is not configured. Exiting.
      ```

b. If you see the following message, Onboard Key Manager (OKM) is configured:

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

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

Go to to complete the recovery process.

c. If you see the following message, External Key Manager (EKM) is configured. Go to the EKM topic and complete the recovery process:

```
Error when fetching key manager config from partner
169.254.139.209: 28
Has key manager been configured on this system? {y|n}
```

3. Monitor the BMR process as it executes restore backup config, env file, mdb, and rdb from the partner.
4. The node reboots and BMR is complete when you see the following:

```
varfs_backup_restore: update checksum for varfs.tgz
varfs_backup_restore: restore using /cfcard/x86_64/freebsd/oldvarfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: Rebooting to load the new varfs
.
Terminated
varfs_backup_restore: bootarg.abandon_varfs is set! Skipping /var
backup.
```

Option 2: Recovery with Onboard Key Manager present

You can restore the ONTAP image (boot media recovery) from the partner node using the `boot_recovery -partner` with ASA r2 platforms running ONTAP 9.16.0 and later.

Before you begin

When you boot a node and the boot media on that node is corrupted, you'll see the following messages and the boot process with stop at the LOADER prompt:

```
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>
```

If you see this message, you must restore the ONTAP image

Steps

1. From the LOADER prompt, enter the *boot_recovery -partner* command.

   The screen will displays the message `Starting boot media recovery (BMR) process press Ctrl-C to abort…` and begins initial checks and installation of the boot recovery files.

   a. If Onboard Key Manager (OKM) is configured, you wil see the following displayed:

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

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

2. Enter *y* at the prompt.
3. Enter the passphrase for onboard key manager when you see `Enter the passphrase for onboard key management:`
4. Enter the pass phrase for onboard key manager again when prompted to confirm the passphrase.

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
Enter the backup data:
TmV0QXBwIEtleSBCbG9iAAECAAAEAAAAcAEAAAAAAAA3yR6UAAAAACEAAAAAAAAA
QAAAAAAAAACJz1u2AAAAAPX84XY5AU0p4Jcb9t8wiwOZoqyJPJ4L6/j5FHJ9yj/w
RVDO1sZB1E4HO79/zYc82nBwtiHaSPWCbkCrMWuQQDsiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAABHVFpxAAAAAHUgdVq0EKNp
.
.
.
.
```

You will see the following when the recovery process is complete:

```
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.
```

5. Monitor the BMR process as it executes restore backup config, env file, mdb, and rdb from the partner.

   When the restore is complete, the node reboots to complete the process.

Option 3: Recovery with External Key Manager present

You can restore the ONTAP image (boot media recovery) from the partner node using the `boot_recovery -partner` with ASA r2 platforms running ONTAP 9.16.0 and later.

When you boot a node and the boot media on that node is corrupted, you'll see the following messages and the boot process with stop at the LOADER prompt:

```
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>
```

If you see this message, you must restore the ONTAP image.

Steps

1. From the LOADER prompt, enter the *boot_recovery -partner* command.

   The screen will displays the message `Starting boot media recovery (BMR) process press Ctrl-C to abort…` and begins initial checks and installation of the boot recovery files.

   a. If External Key Manager (EKM) is configured, you will see the following displayed:

   ```
   Error when fetching key manager config from partner
   169.254.139.209: 28
   Has key manager been configured on this system? {y|n}
   ```

   b. Enter *y* if a key manager has been configured.

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

   Bootmenu Option 11 will prompt the user for all of the EKM configuration information so that the configuration files can be rebuilt.

2. Enter the EKM confiuration at each prompt.

   NOTE: Most of this information was entered when EKM was originally enabled. You should enter the

same information that was entered during initial EKM configuration.

3. Check that the `Keystore UUID` and `Cluster UUID` are correct.
   a. On the partner node retrieve the Cluster UUID with the `cluster identity show` command.
   b. On the partner node retrieve the Keystore UUID with the `vserver show -type admin` command and the `key-manager keystore show -vserver <nodename>` command.
   c. Enter the values for Keystore UUID and Cluster UUID when prompted.

      NOTE: If the partner node is not available, the Keystore UUID and Cluster UUID can be obtained from the Mroot-AK key located on the configured key server.

      Verify the `x-NETAPP-ClusterName: <cluster name>` for the Cluster UUID and `x-NETAPP-KeyUsage: "MROOT-AK"` for the Keystore UUID attributes to ensure you have the correct keys.

4. Monitor the retrieve and restore of Mroot-AK into the ONTAP node.
5. If the process cannot restore the key, you will see the following message and need to configure e0M from the menu system shell:

```
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>
```

   a. Run the `boot_recovery -partner` command on recoverery node.
   b. When prompted to perform (y or n) the options for EKM, select *n* for all.

      After selecting *n* option for the 8 prompts, the system will stop at boot menu.

   c. Collect the /cfcard/kmip/servers.cfg file information from another cluster node. You will collect the following information:
      - The KMIP server address.
      - The KMIP port.
      - The Keystore UUID.

- A copy of the client certificate from the /cfcard/kmip/certs/client.crt file.
- A copy of the client key from the /cfcard/kmip/certs/client.key file.
- A copy of the KMIP server CA(s) from the /cfcard/kmip/certs/CA.pem file.

d. Enter systemshell from bootmenu by entering *systemshell* at the prompt.

e. Configure network from the systemshell menu for e0M, netmask and gateway.

f. Exit from menu systemshell with the *exit* command.

g. You will see the boot menu. Select option `11` to continue EKM restore.

h. Answer `y` to the following questions and enter the required information you previously collected when prompted:

- 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}

6. If the key is restored properly, the recovery process continues and reboots the node.

Return the failed part to NetApp - ASA A1K

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.

Manual method

Boot media replacement workflow - ASA A1K

Follow these workflow steps to replace your boot media.

Review the boot media requirements

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

Check onboard encryption keys

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

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.

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 - ASA A1K

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

Check onboard encryption keys - ASA A1K

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.

Check NVE or NSE

Before shutting down the impaired controller, you need to verify whether the system has security key manager enabled or encrypted disks.

Verify security key-manager configuration

Steps

1. Determine if Key Manager is active with the *security key-manager keystore show* command. For more information, see the security key-manager keystore show MAN page

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 no output is displayed, go to shutdown the impaired controller to shutdown the impaired node.
- If the command displays output, the system has `security key-manager` active and you need to display the `Key Manager` type and status.

2. Display the information for the active `Key Manager` using the *security key-manager key query* command.
   - If the `Key Manager` type displays `external` and the `Restored` column displays `true`, it's safe to shut down the impaired controller.
   - If the `Key Manager` type displays `onboard` and the `Restored` column displays `true`, you need to complete some additional steps.
   - If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `true`, you need to complete some additional steps.
   - If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `true`, you need to complete some additional steps.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays `true`, manually back up the OKM information:
   a. 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. You can safely shut down the impaired controller.
4. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `true`:
   a. Enter the onboard security key-manager sync command: *security key-manager onboard sync*

      Enter the 32 character, alphanumeric onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column displays `true` for all authentication keys: `security key-manager key query`
   c. Verify that the `Key Manager` type displays `onboard`, and then manually back up the OKM information.
   d. Enter the command to display the key management backup information: *security key-manager onboard show-backup*
   e. 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.
   f. You can safely shut down the controller.
5. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `true`:

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 at mysupport.netapp.com.

b. Verify that the `Restored` column displays `true` for all authentication keys: *security key-manager key query*

c. You can safely shut down the impaired controller.

Shut down the impaired controller - ASA A1K

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.

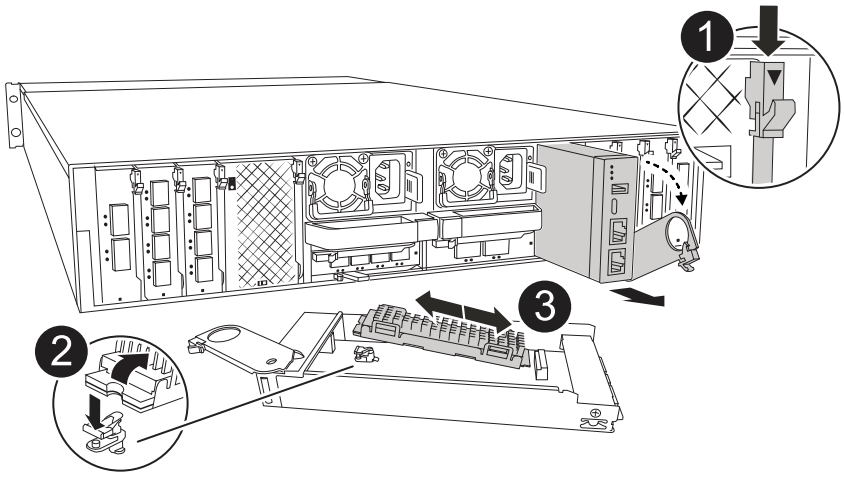
If the impaired controller is displaying…	Then…
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.

Replace the boot media - ASA A1K

To replace the boot media, you must remove the System Management module from the back of the system, remove the impaired boot media, 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.
- You must have 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
  - If NVE is supported, 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.

a. 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 - ASA A1K

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	a. On the impaired controller, press *Y* when you see `Do you want to restore the backup configuration now?` b. On the impaired controller, press *Y* when prompted to overwrite `/etc/ssh/ssh_host_ecdsa_key`. c. On the healthy partner controller, set the impaired controller to advanced privilege level: *set -privilege advanced*. d. On the healthy partner controller, run the restore backup command: *system node restore-backup -node local -target -address impaired_node_IP_address*. **NOTE:** If you see any message other than a successful restore, contact NetApp Support. e. On the healthy partner controller, return the impaired controller 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 the impaired controller and press *ctrl-c* for the Boot Menu. i. If the system does not use encyption, select *Option 1 Normal Boot.*, otherwise go to Restore key managers. j. Connect the console cable to the partner controller. k. Give back the controller using the *storage failover giveback -fromnode local* command. l. Restore automatic giveback if you disabled it by using the *storage failover modify -node local -auto-giveback true* command. m. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the *system node autosupport invoke -node * -type all -message MAINT=END* command. **NOTE:** If the process fails, contact NetApp Support.

If your system is running…	Then…
ONTAP 9.16.1 or later	a. On the impaired controller, press *y* when prompted to restore the backup configuration. After restore procedure is successful, this message will be seen on the console - `syncflash_partner: Restore from partner complete`. b. On the impaired controller, press *y* when prompted to confirm if the restore backup was successful. c. On the impaired controller, press *y* when prompted to use the restored configuration. d. On the impaired controller, press *y* when prompted to reboot the node. e. On the impaired controller, press *y* when prompted to reboot the impaired controller and press *ctrl-c* for the Boot Menu. f. If the system does not use encyption, select *Option 1 Normal Boot.*, otherwise go to Restore key managers. g. Connect the console cable to the partner controller. h. Give back the controller using the *storage failover giveback -fromnode local* command. i. Restore automatic giveback if you disabled it by using the *storage failover modify -node local -auto-giveback true* command. j. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the *system node autosupport invoke -node * -type all -message MAINT=END* command. **NOTE:** If the process fails, contact NetApp Support.

Restore encryption - ASA A1K

Restore encryption on the replacement boot media.

Step 1: Restore onboard key manager

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 or external 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. Select one of the following options to restore the onboard key manager configuration from the ONATP boot menu.

Option 1: Systems with onboard key manager server configuration

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

Before you begin

You need the 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. From the ONTAP boot menu select option 10:

```
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
```

2. Confirm the continuation of the process. `This option must be used only in disaster recovery procedures. Are you sure? (y or n): y`
3. Enter the cluster-wide passphrase twice.

   While entering the passphrase the console will not show any input.

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

4. Enter the backup information. Paste the entire content from the BEGIN BACKUP line through the END BACKUP line.

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

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------END BACKUP---------------------------
```

5. The recovery process will be completed.

```
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.

```
*******************************************************************************
* 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 `Waiting for giveback…(Press Ctrl-C to abort wait)`

8. From the partner node, giveback the partner controller: *storage failover giveback -fromnode local -only-cfo-aggregates true*
9. Once booted only with CFO aggregate run the *security key-manager onboard sync* command:
10. Enter the cluster-wide passphrase for the Onboard Key Manager:

```
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.
```

11. Ensure that all keys are synced: *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 of the node from the partner: *storage failover giveback -fromnode local*

Option 2: Systems with external key manager server configuration

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

Before you begin

You need the following information for restoring the external key manager (EKM) configuration:

- You need 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. Select Option 11 from the ONTAP 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
```

2. When prompted confirm you have gathered the required information:
   a. `Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}` *y*
   b. `Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}` *y*
   c. `Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}` *y*
   d. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *y*

      You may also these prompts instead:

   e. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *n*
      i. `Do you know the KMIP server address? {y/n}` *y*
      ii. `Do you know the KMIP Port? {y/n}` *y*
3. Supply the information for each of these prompts:
   a. `Enter the client certificate (client.crt) file contents:`
   b. `Enter the client key (client.key) file contents:`
   c. `Enter the KMIP server CA(s) (CA.pem) file contents:`
   d. `Enter the server configuration (servers.cfg) file contents:`

```
Example

Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoU1eajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlbkIb4bAgLztHEmUDOkGmXYAkblQ=
-----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
```

4. The recovery process will complete:

```
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.

```
**********************************************************************
***************
* 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
```

Step 2: Complete the boot media replacement

Complete the boot media replacement process after the normal boot by completing final checks and giving back storage.

1. Check the console output:

If the console displays…	Then…
The login prompt	Go to Step 6.
Waiting for giveback…	a. Log into the partner controller. b. Confirm the target controller is ready for giveback with the *storage failover show* command.

2. 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* 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 the partner is "not ready", wait 5 minutes for the HA subsystem to synchronize between the partners.

- If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

3. Wait 3 minutes and check the failover status with the *storage failover show* command.
4. At the clustershell prompt, enter the *network interface 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.

5. Move the console cable to the target controller and run the *version -v* command to check the ONTAP versions.
6. Use the `storage encryption disk show` to review the output.
7. 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 synchronize the missing onboard keys on the repaired node.

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

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

Return the failed part to NetApp - ASA A1K

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