Boot media - automated recovery

Install and maintain

NetApp
October 30, 2024

Table of Contents

Boot media - automated recovery

Overview of automated boot media recovery - ASA A1K

You can replace a failed boot media through the automated boot media replace (BMR) option.

Automated boot media replace 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.

Boot media replacement workflow - ASA A1K

Follow these workflow steps to replace your boot media.

1. **Review the boot media requirements**

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

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 System Management module and install the replacement boot media.

4. **Restore the image on the boot media (automated boot recovery)**

Restore the ONTAP image from the partner controller.

5. **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:

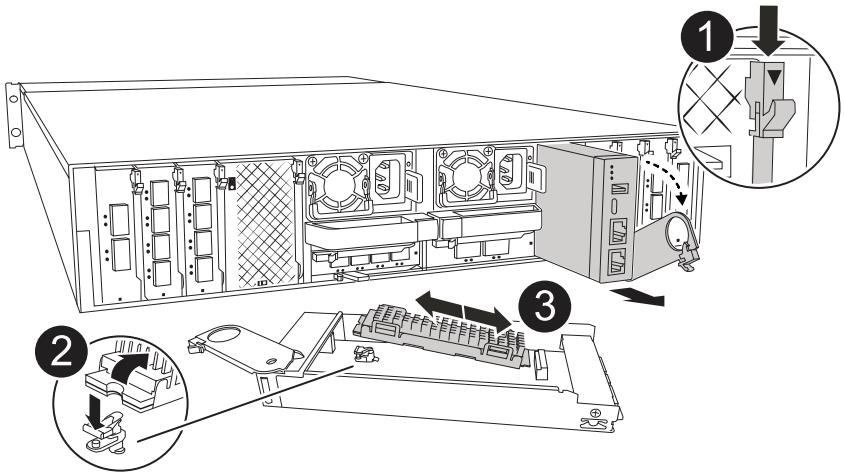
If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*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

Restore the ONTAP image from the partner node when the boot media is corrupted.

About this task

If a node's boot media is corrupted, the boot process will halt at the LOADER prompt and display boot error messages.

When you encounter these boot error messages, you need to restore the ONTAP image from the partner node.

Show example of boot error messages

```
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>
```

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 recovery process as LOADER configures the local cluster ports and executes `netboot` from the partner node.

   When netboot is running, the `Starting BMR` message displays.

3. Depending on the encryption method, select the option that matches your single-node configuration:

No Encryption

If no encryption is detected, the boot media recovery process continues without requiring key management.

Continue to monitor the recovery process as it restores the backup config, env file, mdb, and rdb from the partner node.

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

```
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.
```

Onboard Key Manager (OKM)

If Onboard Key Manager (OKM) is detected, the system displays the following prompt.

```
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. From the Bootmenu Option prompt, enter `Y` to confirm you want to use the bootmedia recovery option.
b. Enter the passphrase for onboard key manager when prompted, and enter the passphrase again to confirm.

Show example of passphrase prompts

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
Enter the backup data:
TmV0QXBwIEtleSBCbG9iAAECAAAEAAAAcAEAAAAAAAA3yR6UAAAAACEAAAAAAA
AA
QAAAAAAAAACJz1u2AAAAAPX84XY5AU0p4Jcb9t8wiwOZoqyJPJ4L6/j5FHJ9yj
/w
RVDO1sZB1E4HO79/zYc82nBwtiHaSPWCbkCrMWuQQDsiAAAAAAAAACgAAAAAAA
AA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAA
AA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LR
zU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAABHVFpxAAAAAHUgdVq0EK
Np
.
.
.
.
```

c. Continue to monitor the recovery process as it restores the backup config, env file, mdb, and rdb 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.wkeydb file.

Successfully recovered keymanager secrets.
```

External Key Manager (EKM)

If EKM is configured, the system displays the following prompt.

```
Error when fetching key manager config from partner <IP>: 28

Has key manager been configured on this system? {y|n}
```

a. Enter `Y` if EKM has been configured.

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

You'll be prompted for the EKM settings that were initially used during setup.

b. Enter each EKM configuration setting when prompted.

c. Verify that the attributes for the Cluster UUID and the Keystore UUID are correct.

- On the partner node, retrieve the Cluster UUID using the following command.

  ```
  cluster identity show
  ```

- On the partner node, retrieve the Keystore UUID using the following commands.

  ```
  vserver show -type admin
  ```

  ```
  key-manager keystore show -vserver <nodename>
  ```

- If the partner node is unavailable, use the Mroot-AK key to retrieve the UUID:
  - For the Cluster UUID, enter the following command:

    ```
    x-NETAPP-ClusterName: <cluster name>
    ```

  - For the Keystore UUID, enter the following command:

    ```
    x-NETAPP-KeyUsage: MROOT-AK
    ```

d. Enter the values for Keystore UUID and Cluster UUID when prompted.

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

- If the key is successfully restored, the recovery process continues and reboots the node. Proceed to step 4.
- If the key is not successfully restored, the system will halt and display error and warning messages. Rerun the recovery process.

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.

System cannot connect to key managers.

ERROR: kmip_init: halting this system with encrypted
mroot...

Terminated

Uptime: 11m32s

System halting...

LOADER-B>
```

4. When the node reboots, verify the boot media recovery was successful by confirming that the system is back online and operational.
5. Return the impaired controller to normal operation by giving back its storage:

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

6. If automatic giveback was disabled, reenable it:

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

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

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

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