Automated method

Install and maintain

NetApp
September 25, 2024

Table of Contents

Automated method

Boot media replacement workflow - ASA A70 and ASA A90

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 image on 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.

Requirements and considerations - ASA A70 and ASA A90

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 controller - ASA A70 and ASA A90

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:

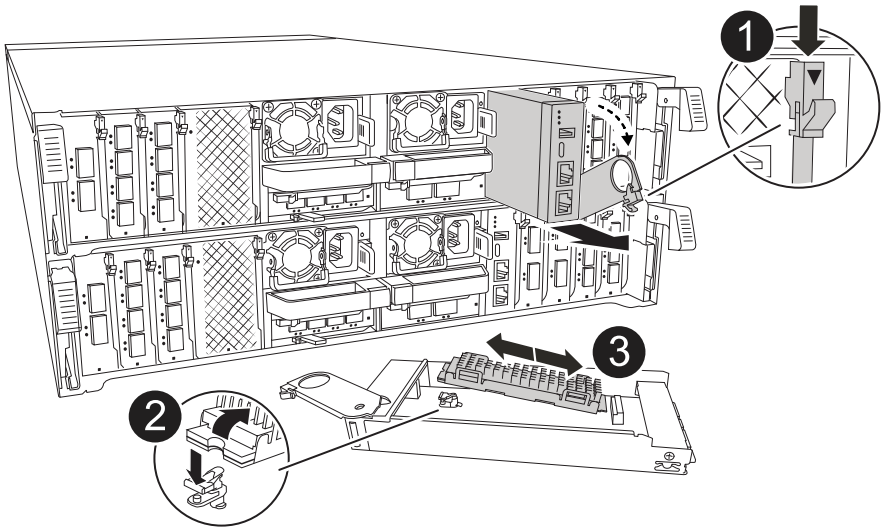
If the impaired controller is displaying…	Then…
The LOADER prompt	Go to the next step.
Waiting for giveback…	Press Ctrl-C, and then respond `y` when prompted.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*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

Replace the boot media - ASA A70 and ASA A90

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

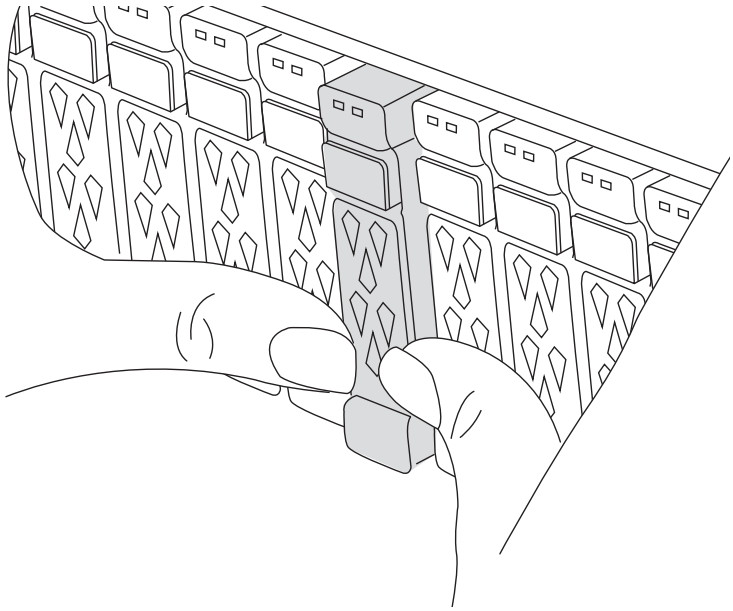
Steps

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. On the front of the chassis, use your thumbs to firmly push each drive in until you feel a positive stop. This ensures that the drives are firmly seated against the chassis midplane.



2. Go to the rear of the chassis. If you are not already grounded, properly ground yourself.

3. Disconnect power to the controller module by pulling the controller module out about three inches:
    a. Press down on both of the controller module locking latches, and then rotate both latches downward at the same time.
    b. Pull the controller module about 3 inches out of the chassis to disengage power.
    c. Remove any cables connected to the System Management module. Make sure to label where the cables were connected, so that you can connect them to the correct ports when you reinstall the module.
    d. 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.
    e. Depress the system management cam button. The cam lever moves away from the chassis.
    f. Rotate the cam lever all the way down and remove the System Management module from the controller module.
    g. Place the System Management module on an anti-static mat, so that the boot media is accessible.
4. 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.
5. 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.
6. Reinstall the System Management module:
    a. Rotate the cable management tray up to the closed position.
    b. Recable the System Management module.

Automated boot recovery - ASA A70 and ASA A90

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 A70 and ASA A90

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