NetApp

Controller

Install and maintain

NetApp
December 18, 2024

Table of Contents

Controller

Controller replacement workflow - ASA A1K

Follow these workflow steps to replace your controller module.

1 **Review controller replacement requirements**

To replace the controller module, 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 controller**

Replacing the controller includes removing the impaired controller, moving the FRU components to the replacement controller module, and then installing the replacement controller module in the enclosure.

4 **Restore and verify the system configuration**

Verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

5 **Give back the controller**

Transfer the ownership of storage resources back to the replacement controller.

6 **Complete controller replacement**

Verify the LIfs, check cluster health, and return the failed part to NetApp.

Controller replace requirements - ASA A1K

Review the requirements for the controller replacement procedure and select the correct one for your version of the ONTAP operating system.

- All drive shelves must be working properly.
- The healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the "impaired controller").
- You must replace the failed component with a replacement FRU component you received from your provider.
- You must replace a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.

- You cannot change any drives or drive shelves as part of this procedure.

- Because the boot device is located on the System Management module that is installed in the back of the system, you do not need to move the boot device when replacing a controller module.

- It is important that you apply the commands in these steps on the correct systems:

  - The *impaired* controller is the controller that is being replaced.

  - The *replacement* controller is the new controller that is replacing the impaired controller.

  - The *healthy* controller is the surviving controller.

- You must always capture the controller's console output to a text log file.

  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Shut down the impaired controller - ASA A1K

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 controller module hardware - ASA A1K

To replace the controller, you must remove the impaired controller, move FRU components to the replacement controller module, install the replacement controller module in the enclosure, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

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

1. Check the NVRAM status LED located in slot 4/5 of the system. There is also an NVRAM LED on the front panel of the controller module. Look for the NV icon:
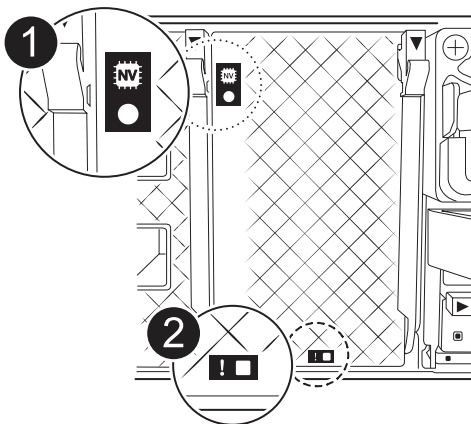

❶	NVRAM status LED
❷	NVRAM attention LED

  ◦ If the NV LED is off, go to the next step.

- If the NV LED is flashing, wait for the flashing to stop. If flashing continues for longer than 5 minutes, contact Technical Support for assistance.

2. If you are not already grounded, properly ground yourself.

3. On the front of the unit, hook your fingers into the holes in the locking cams, squeeze the tabs on the cam levers, and gently, but firmly rotate both latches toward you at the same time.

   The controller module moves slightly out of the enclosure.
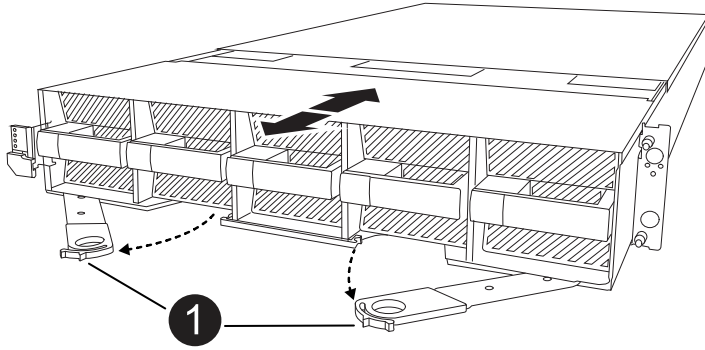
	Locking cam latches

4. Slide the controller module out of the enclosure and place it on a flat, stable surface.

   Make sure that you support the bottom of the controller module as you slide it out of the enclosure.

Step 2: Move the fans

You must remove the five fan modules from the impaired controller module to the replacement controller module.

1. If you are not already grounded, properly ground yourself.

2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.

3. Press the gray locking button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.

   (i) The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.
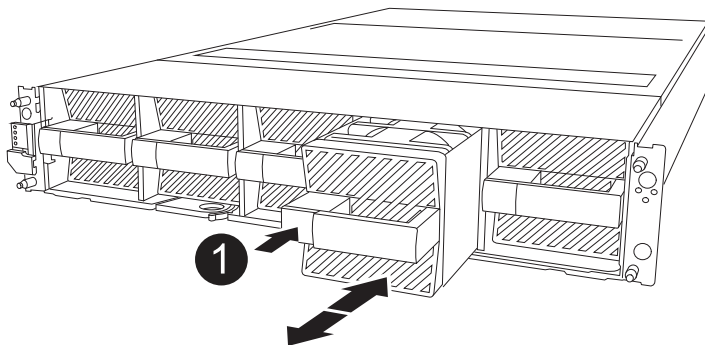
❶	Black locking button

4. Install the fan in the replacement controller module:

   a. Align the edges of the fan housing with the opening in the front of the replacement controller module.

   b. Gently slide the fan module all the way into the replacement controller module until it locks in place.

5. Repeat the preceding steps for the remaining fan modules.

Step 3: Move the NV battery

Move the NV battery to the replacement controller.

1. Open the NV battery air duct cover and locate the NV battery.
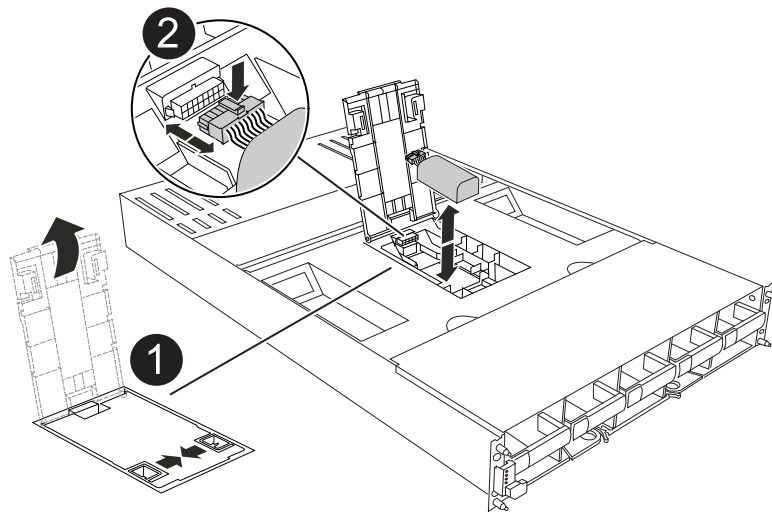
|	
❶	NV battery air duct cover
❷	NV battery plug
❸	NV battery pack

2. Lift the battery up to access the battery plug.

3. Squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.

4. Lift the battery out of the air duct and controller module.

5. Move the battery pack to the replacement controller module and then install it in the NV battery air duct:

   a. Open the NV battery air duct in the replacement controller module.

   b. Plug the battery plug into the socket and make sure that the plug locks into place.

   c. Insert the battery pack into the slot and press firmly down on the battery pack to make sure that it is locked into place.

   d. Close the air duct cover.

Step 4: Move system DIMMs

Move the DIMMs to the replacement controller module.

1. Open the motherboard air duct and locate the DIMMs.
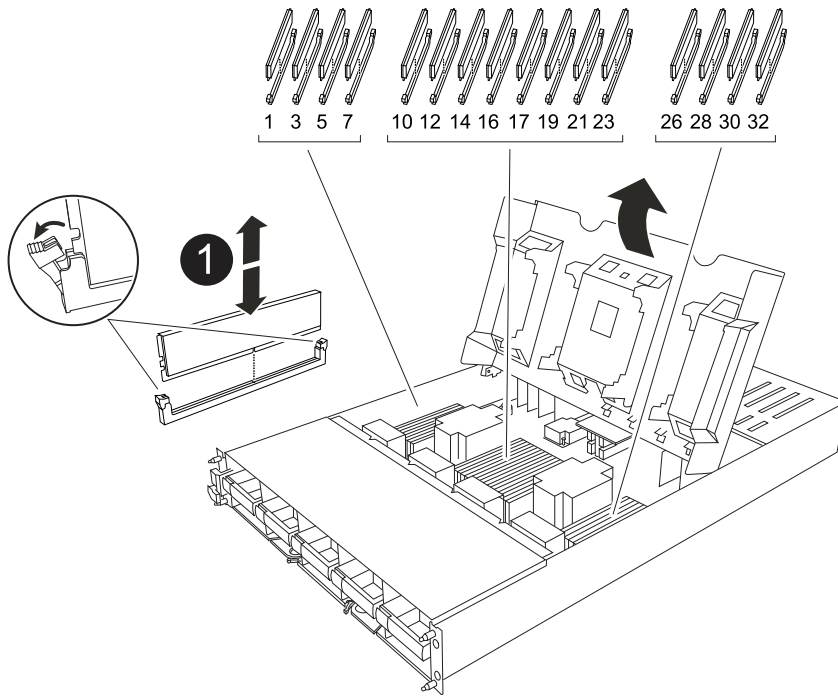
1	System DIMM

2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.

3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

   (i) Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

4. Locate the slot where you are installing the DIMM in the replacement controller module.

5. Insert the DIMM squarely into the slot.

   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

   (i) Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

6. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

7. Repeat these steps for the remaining DIMMs. Close the motherboard air duct.

Step 5: Install the controller module

Reinstall the controller module and boot it.

1. Ensure the air duct is completely closed by rotating it down as far as it will go.

   It must lie flush against the controller module sheet metal.

2. Align the end of the controller module with the opening in the enclosure, and slide the controller module into the chassis with the levers rotated away from the front of the system.

3. Once the controller module stops you from sliding it farther, rotate the cam handles inward until they latch back under the fans

   > (i) Do not use excessive force when sliding the controller module into the enclosure to avoid damaging the connectors.

   > (i) The controller boots to the LOADER prompt as soon as it is fully seated.

4. From the LOADER prompt, enter `show date` to display the date and time on the replacement controller. Date and time are in GMT.

   > (i) Time displayed is local time not always GMT and is displayed in 24hr mode.

5. Set the current time in GMT with the `set time hh:mm:ss` command. You can get the current GMT from the partner node the `date -u`command.

6. Recable the storage system, as needed.

   If you removed the transceivers (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

Restore and verify the system configuration - ASA A1K

After completing the hardware replacement, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Verify HA config settings

You must verify the `HA` state of the controller module and, if necessary, update the state to match your system configuration.

1. Boot to maintenance mode: `boot_ontap maint`

   a. Enter `y` when you see *Continue with boot?*.

      If you see the *System ID mismatch* warning message, enter `y`.

2. Enter `sysconfig -v` and capture the display contents.

   > (i) if you see *PERSONALITY MISMATCH* contact customer support.

3. From the `sysconfig -v` output, compare the adapter card information with the cards and locations in the replacement controller.

4. Verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

5. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`

   The value for HA-state can be one of the following:

   ◦ `ha`

   ◦ `mcc` (not supported)

   ◦ `mccip` (not supported in ASA systems)

   ◦ `non-ha` (not supported)

6. Confirm that the setting has changed: `ha-config show`

Step 2: Verify disk list

1. Verify that the adapter lists the paths to all disks with the `storage show disk -p`.

   If you see any issues, check cabling and reseat cables.

2. Exit Maintenance mode: `halt.`

Give back the controller - ASA A1K

Verify the storage and network connections, and then give back the controller.

Give back the controller

Reset encryption if enabled and return the controller to normal operation.

No encryption

1. From the LOADER prompt, enter `boot_ontap`.

2. Press <enter> when console messages stop.

   ◦ If you see the *login* prompt, go to the next step at the end of this section.

   ◦ If you see *Waiting for giveback*, press the <enter> key, log into the partner node, and then go to the next step at the end of this section.

3. Return the impaired controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *impaired_node_name.*

4. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`.

5. If AutoSupport is enabled, restore/unsuppress automatic case creation: `system node autosupport invoke -node * -type all -message MAINT=END`.

Onboard encryption (OKM)

1. From the LOADER prompt, enter `boot_ontap maint`.

2. Boot to the ONTAP menu from the LOADER prompt `boot_ontap menu` and select option 10.

3. Enter the OKM passphrase. You can get this passphrase from the customer, or contact NetApp Support.

   > (i) You will be prompted twice for the passphrase.

4. Enter the backup key data when prompted.

5. At the boot menu, enter option `1` for normal boot.

6. Press <enter> when *Waiting for giveback* is displayed.

7. Move the console cable to the partner node and login as `admin`.

8. Ensure any core dumps on the repaired node are saved by going to advanced mode" `set -privilege advanced` and then `run local partner savecore`.

9. Return to admin lever: `set privilege admin`.

10. Give back only the CFO aggregates (the root aggregate): `storage failover giveback -fromnode local -only-cfo-aggregates true`

    ◦ If you encounter errors, contact NetApp Support.

11. Wait 5 minutes after the giveback report completes, and check failover status and giveback status: `storage failover show` and `storage failover show-giveback`.

12. Move the console cable to the replacement node and enter `security key-manager onboard sync`

    > (i) You will be prompted for the cluster-wide passphrase of OKM for the cluster.

13. Check status of the keys with the following command: `security key-manager key query -key -type svm-KEK`.

    If the *Restored* column shows anything but *true*, contact NetApp Support.

14. Return the impaired controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *impaired_node_name*.

15. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`.

16. If AutoSupport is enabled, restore/unsuppress automatic case creation: `system node autosupport invoke -node * -type all -message MAINT=END`.

External key manager (EKM))

1. If the root volume is encrypted with External Key Manager and the console cable is connected to the replacement node, enter `boot_ontap menu` and select option `11`.

2. Answer `y` or `n` to the following questions:

   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}

   OR

   Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}

   Do you know the KMIP server address? {y/n}

   Do you know the KMIP port? {y/n}

   > ⓘ　Contact NetApp Support if you have issues.

3. Supply the information for:
   ◦ The client certificate (client.crt) file contents.
   ◦ The client key (client.key) file contents.
   ◦ The KMIP server CA(s) (CA.pem) file contents.
   ◦ The IP address for the KMIP server.
   ◦ The port for the KMIP server.

4. Once the system processes, you will see the Boot Menu. Select '1' for normal boot.

5. Check the takeover status: `storage failover show`.

6. Ensure any core dumps on the repaired node are saved by going to advanced mode" `set -privilege advanced` and then `run local partner savecore`.

7. Return the impaired controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *impaired_node_name*.

8. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`.

9. If AutoSupport is enabled, restore/unsuppress automatic case creation: `system node autosupport invoke -node * -type all -message MAINT=END`.

Complete controller replacement - ASA A1K

To restore your system to full operation, you must verify the LIfs, check cluster health, and return the failed part to NetApp.

Step 1: Verify LIFs and and check cluster health

Before returning the *replacement* node to service, you should verify that the LIFs are on their home ports, check the cluster health, and reset automatic giveback.

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

   If any LIFs are listed as false, revert them to their home ports: `network interface revert -vserver * -lif *`

2. Check the health of your cluster. See the How to perform a cluster health check with a script in ONTAP KB article for more information.

3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

Step 2: Return the failed part to NetApp

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.