Replacing the controller module

To replace a controller module, you must remove the impaired node from the system and move the replaceable components from the impaired node to the replacement node. You then install the replacement node in the system chassis.

Before you begin

- All disk shelves must be working properly.
- If your system is in an HA pair, the healthy node must be able to take over the node that is being replaced (referred to in this procedure as the impaired node).

About this task

- This procedure is for systems running ONTAP 8.2 and later only.
- This procedure includes steps for automatically or manually reassigning disks to the *replacement* node, depending on your system's configuration.
  You should be sure to perform the disk reassignment as directed in the procedure.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing 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 disks or disk shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired node to the replacement node so that the replacement node will boot up in the same version of ONTAP as the old controller.
- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* node is the node that is being replaced.
  - The *replacement* node is the new node that is replacing the impaired node.
  - The *healthy* node is the surviving node.

Choices

- Replacing a controller module in 7-Mode environments on page 1
- Replacing a controller module in ONTAP on page 26

Replacing a controller module in 7-Mode environments

You must follow a specific series of steps to replace the for your mode and version of ONTAP.

Steps

1. Pre-replacement tasks for SAN configurations on page 2
2. Pre-replacement tasks for Storage Encryption configurations on page 3
3. Shutting down a node running Data ONTAP operating in 7-Mode on page 4

Pre-replacement tasks for SAN configurations

If you have a SAN configuration, you must save the FC port configuration information of the impaired node so that you can reenter it on the replacement node .

About this task

Your system configuration determines your access to port configuration information.

Step

1. Take one of the following actions, depending on your configuration:

If the system is in...	Then...
A stand-alone configuration and is not running	You have to rely on any configuration backups or information gathered previously from the AutoSupport tool.
An HA pair and the impaired node has not been taken over by the healthy node and is running	**a.** To save the port configuration information for the impaired node: **`fcadmin config`** **b.** Copy and save the screen display to a safe location for later reuse. **Note:** If the impaired node is taken over by its partner, you can boot it to Maintenance mode and run the `fcadmin config` command in Maintenance mode. To boot the impaired node to Maintenance mode, restart the impaired node, press Ctrl-C to interrupt the boot process when you see the message `Press Ctrl-C` for the Boot Menu. From the Boot Menu, enter the option for Maintenance mode. **c.** Enter the `Cluster-Mode` command to save the port configuration information for the impaired node: **`fcadmin config`**

Pre-replacement tasks for Storage Encryption configurations

If the storage system whose controller you are replacing is configured to use Storage Encryption, you must first reset the authentication keys of the disks to their MSID (the default security ID set by the manufacturer). This is a temporary necessity during the controller replacement process to avoid any chance of losing access to the data.

About this task

After resetting the authentication keys to the MSID, the data on the disks is no longer encrypted with secret authentication keys. You must verify the physical safety of the disks during the replacement or upgrade process.

Steps

1. Display the key ID for each self-encrypting disk on the original system:

   `disk encrypt show`

   #### Example

   ```
   disk encrypt show
   Disk       Key ID                                                           Locked?
   0c.00.1    0x0                                                              No
   0c.00.0    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
   0c.00.3    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
   0c.00.4    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
   0c.00.2    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
   0c.00.5    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
   ```

   The first disk in the example is associated with an MSID; the others are associated with a non-MSID.

2. Examine the output of the `disk encrypt show` command, and if any disks are associated with a non-MSID key, rekey them to an MSID key by taking one of the following actions:

   - Rekey the disks individually, once for each disk:

     `disk encrypt rekey 0x0 disk_name`

   - Rekey all the disks at once:

     `disk encrypt rekey 0x0 *`

3. Verify that all the self-encrypting disks are associated with an MSID:

   `disk encrypt show`

   #### Example

   The following example shows the output of the `disk encrypt show` command when all self-encrypting disks are associated with an MSID:

   ```
   cluster::> disk encrypt show
   Disk       Key ID                                                           Locked?
   ---------- ---------------------------------------------------------------- -------
   0b.10.23   0x0                                                              No
   0b.10.18   0x0                                                              No
   0b.10.0    0x0                                                              Yes
   0b.10.12   0x0                                                              Yes
   0b.10.3    0x0                                                              No
   0b.10.15   0x0                                                              No
   0a.00.1    0x0                                                              Yes
   0a.00.2    0x0                                                              Yes
   ```

Shutting down a node running Data ONTAP operating in 7-Mode

When performing maintenance on a system running Data ONTAP operating in 7-Mode, you must shut down the node. Depending on your system's configuration, you might also need to turn off the power supplies.

About this task

Your system's configuration determines whether you turn off the power supplies after shutting down the node:

- If you have one controller module in a stand-alone configuration, you must turn off the power supplies in the impaired node chassis.

Shutting down a node in an HA pair

To shut down the node, you must determine the status of the node and, if necessary, take over the node so that the partner continues to serve data from the node's storage.

Steps

1. Check the HA status of the impaired node from either node in the HA pair that is displaying the ONTAP prompt:

   `cf status`

2. Take the appropriate action based on the takeover status of the node.

If the impaired node...	Then...
Has been taken over by the healthy node and is halted	Go to the next step.
Has not been taken over by the healthy node and is running	Take over the impaired node from the prompt of the healthy node: **`cf takeover`**

3. Wait for two minutes after takeover of the impaired node to confirm that the takeover was completed successfully.

4. With the impaired node showing the `Waiting for giveback` message or halted, shut it down, depending on your configuration:

If the Service Processor (SP)...	Then...
Is configured	Log in to the SP, and then turn off the power: **`system power off`**
Is not configured	At the prompt of the impaired node, press Ctrl-C and respond **`Y`** to halt the node.

Shutting down a node in a stand-alone configuration

For a node that is not configured with a high-availability (HA) partner, you must perform a clean shutdown (verifying that all data has been written to disk) and disconnect the power supplies.

Steps

1. Shut down the node if it is not already shut down:

   `halt -t 0`

2. Shut down the power supplies, and then unplug both power cords from the source.

   The system is ready for maintenance.

Removing the controller module and moving the components

You must remove the old controller module from the chassis and move all field-replaceable components from the old controller module to the new controller module.

About this task

Attention: If the system is in an HA pair, you must wait for two minutes after takeover of the impaired node to confirm that the takeover was successfully completed before removing the controller module.

To reduce the possibility of damage to the replaceable components, you should minimize handling by installing the components into the new controller module as soon as you remove them from the old controller module.

Steps

1. Removing the controller module from the system on page 5
2. Moving the mezzanine card on page 7
3. Moving the boot device on page 8
4. Moving the NVMEM battery on page 9
5. Moving the DIMMs to the new controller module on page 10

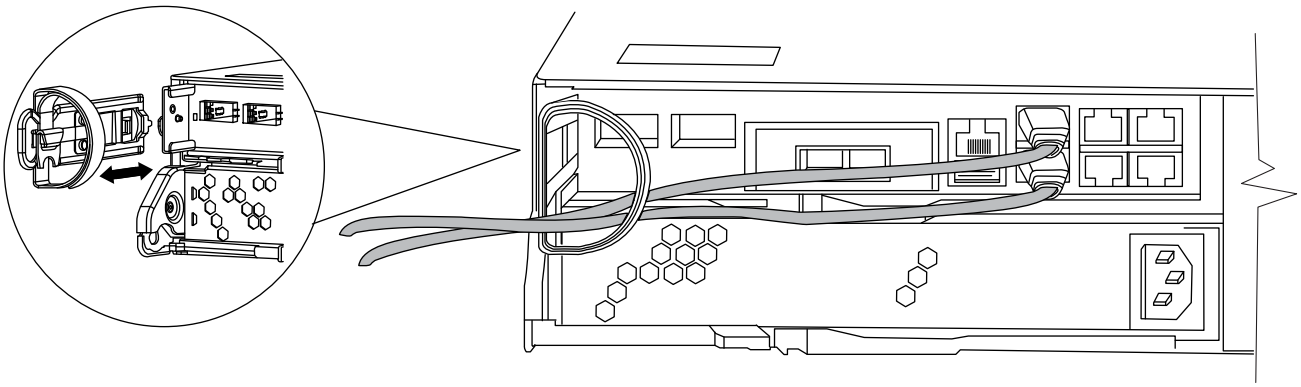
Removing the controller module from the system

To replace the controller module, you must first remove the old controller module from the system.

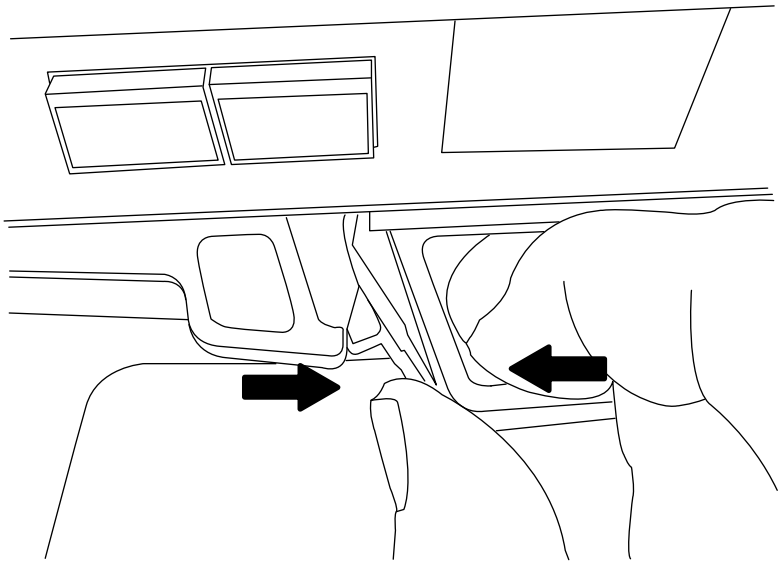
Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management arm, and then unplug the system cables and SFPs (if needed) from the controller module, and keep track of where the cables were connected.

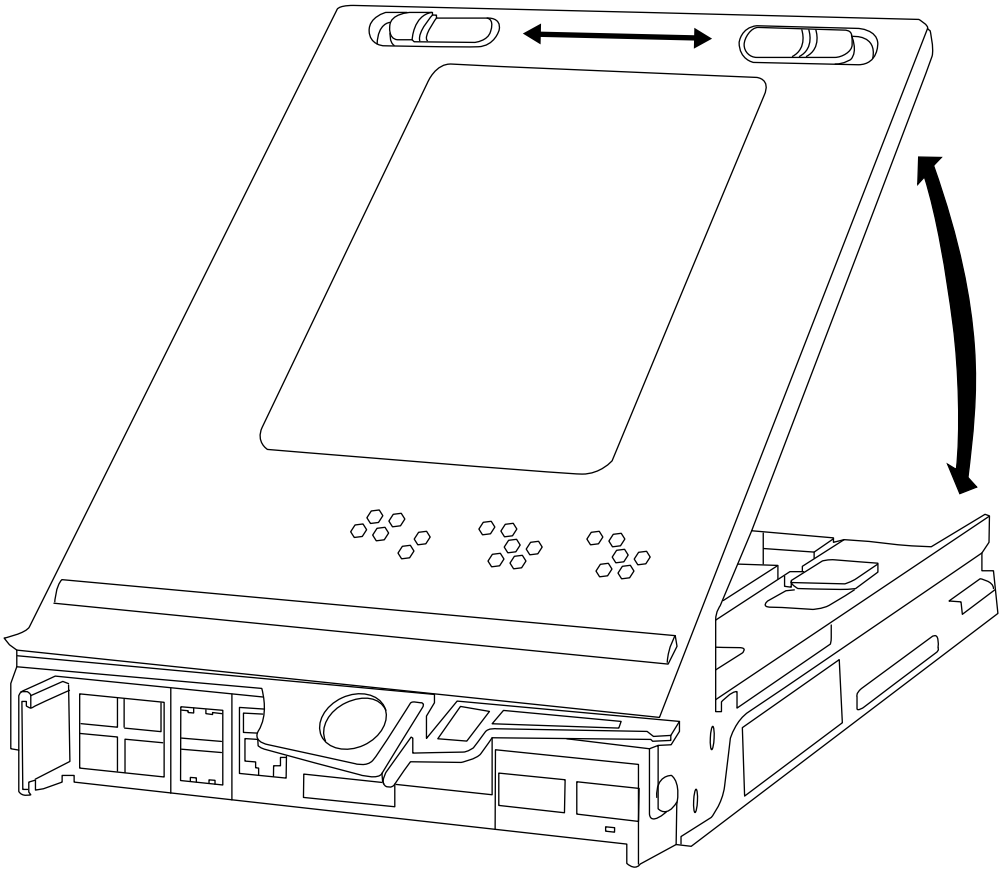
   Leave the cables in the cable management arm so that when you reinstall the cable management arm, the cables are organized.
3. Remove the cable management arms from the left and right sides of the controller module and set them aside.



   The illustration shows a FAS2220 or FAS2240-2 system. The procedure is the same for all FAS22xx systems.
4. Squeeze the latch on the cam handle until it releases, as shown in the following illustration. Open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and open it by sliding the blue tabs to release the cover, and then swing the cover up and open.

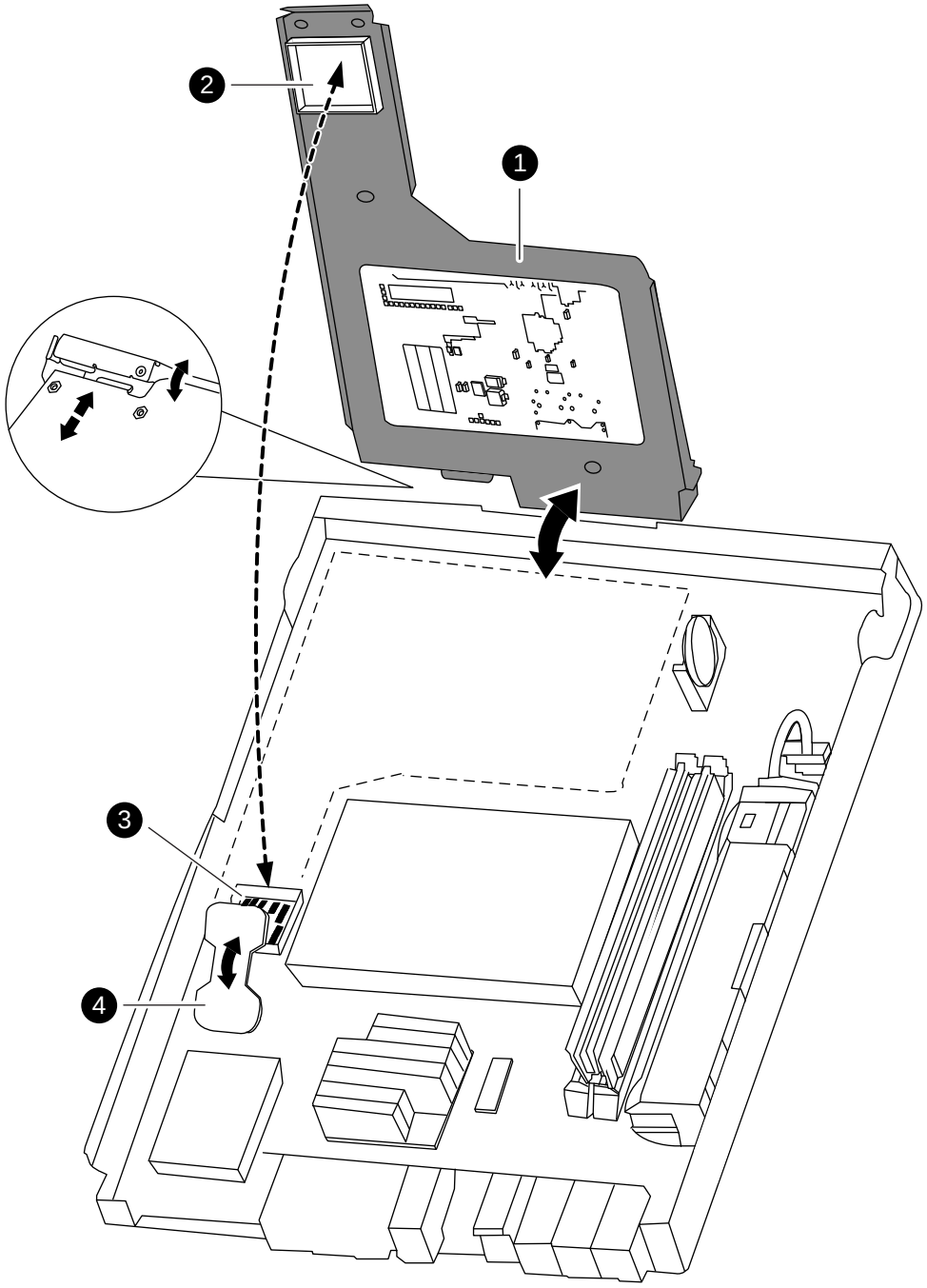


Moving the mezzanine card

If the system has a mezzanine card, you must move it from the old controller module to the new controller module to maintain airflow requirements or the selected I/O functionality.

Steps

1. Release the lever that holds the mezzanine blank or card in place.



1	Mezzanine card

2	Mezzanine card connector
3	Motherboard socket for mezzanine card connector
4	Lever (when closed, engages and locks the mezzanine card connector in the socket)

Note: The illustration shows a mezzanine card; the mezzanine blank does not have the circuit board.

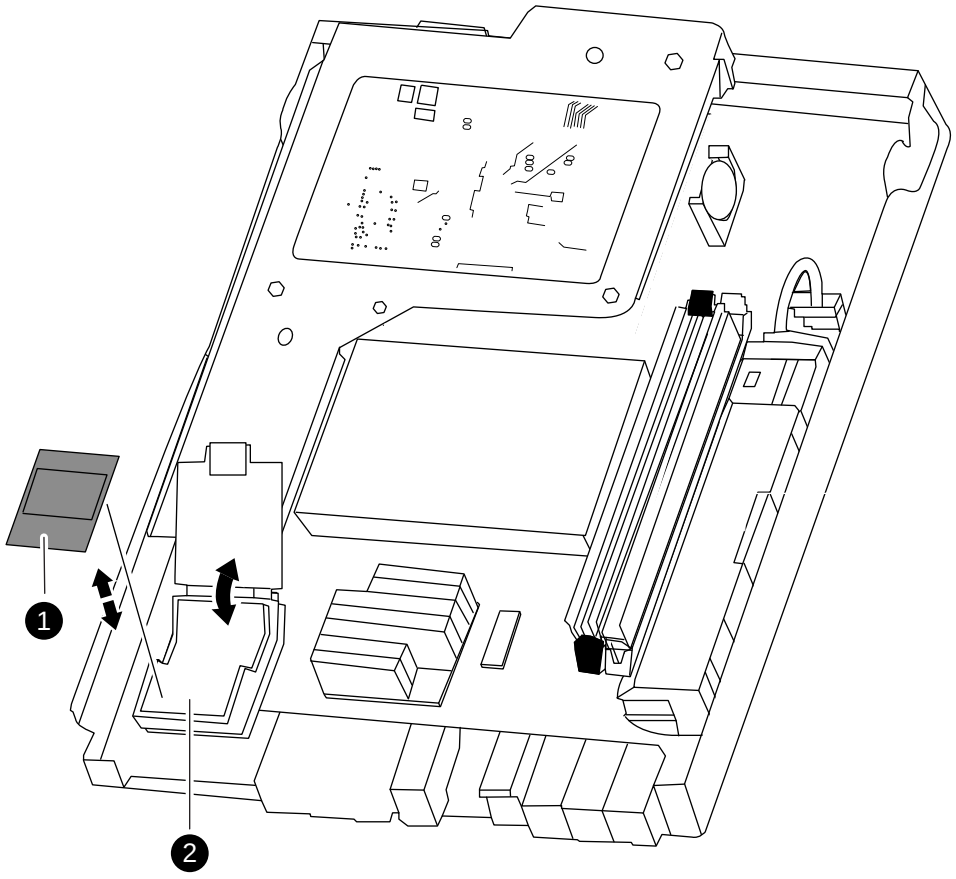
2. Swing the mezzanine blank or card up and lift it out of the controller module.
3. Align the mezzanine blank or card I/O panel in the slot in the front of the new controller module, and swing the mezzanine blank or card down to seat the connector into the socket on the controller module.
4. Close and push down on the blue lever to engage the mezzanine blank or card connector and to secure the mezzanine blank or card.

Moving the boot device

To move the boot device from the old controller module to the new controller module, you must perform a specific sequence of steps.

Steps

1. Locate the boot device using the following illustration or the FRU map on the controller module:



1	Boot device
2	Boot device holder; not removable

2. Open the boot device cover and hold the boot device by its edges at the notches in the boot device housing, gently lift it straight up and out of the housing.

   Attention: Always lift the boot device straight up out of the housing. Lifting it out at an angle can bend or break the connector pins in the boot device.

3. Open the boot device cover on the new controller module.
4. Align the boot device with the boot device socket or connector, and then firmly push the boot device straight down into the socket or connector.

   Important: Always install the boot device by aligning the front of the boot device squarely over the pins in the socket at the front of the boot device housing. Installing the boot device at an angle or over the rear plastic pin first can bend or damage the pins in the boot device connector.

5. Check the boot device to make sure that it is seated squarely and completely in the socket or connector.

   If necessary, remove the boot device and reseat it into the socket.

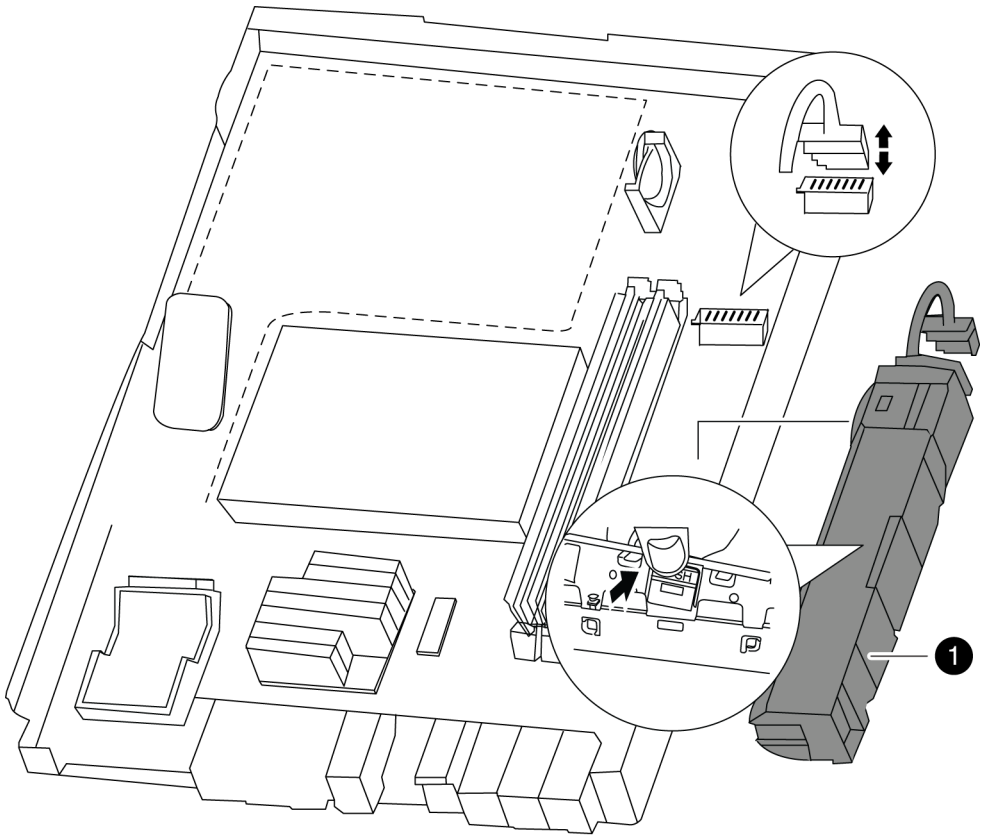
6. Close the boot device cover.

Moving the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

Steps

1. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.



1	NVMEM battery

2. Grasp the battery and press the tab marked PUSH, and then lift the battery out of the holder and controller module.
3. In the new controller module, seat the battery in the holder.

   Attention: Do not connect the NVMEM keyed battery plug into the socket until after the NVMEM DIMM has been installed.

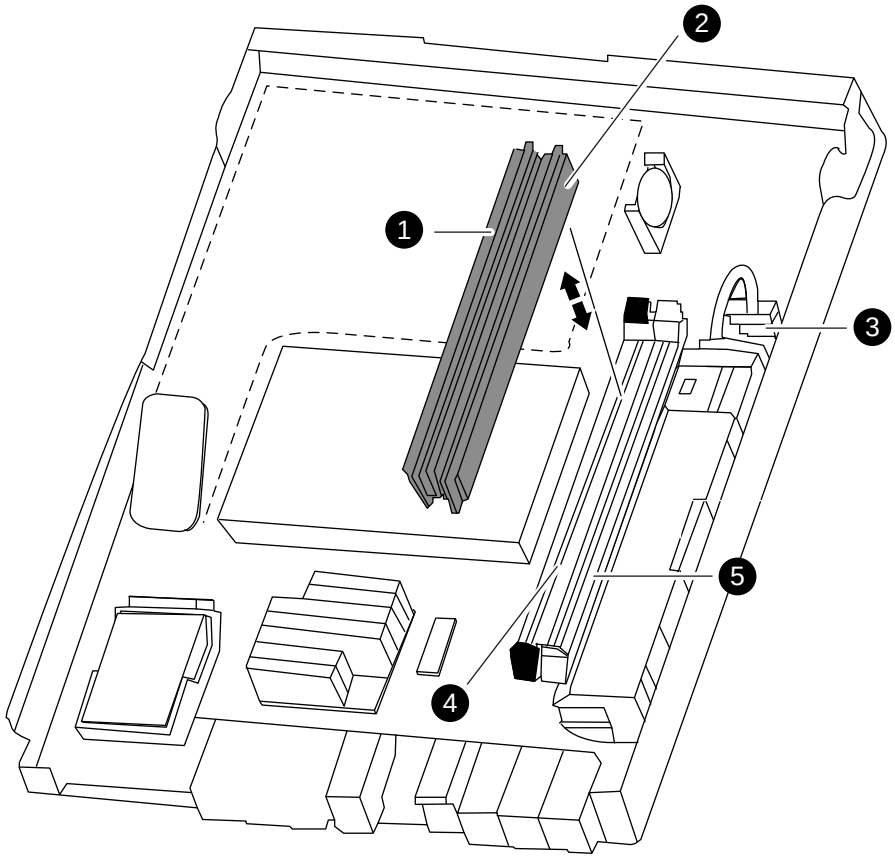
Moving the DIMMs to the new controller module

You must remove the DIMMs from the old controller module, being careful to note their locations so that you can reinstall them in the correct sockets in the new controller module.

Steps

1. Verify that the NVMEM battery cable connector is not plugged into the socket .
2. Locate the DIMMs.

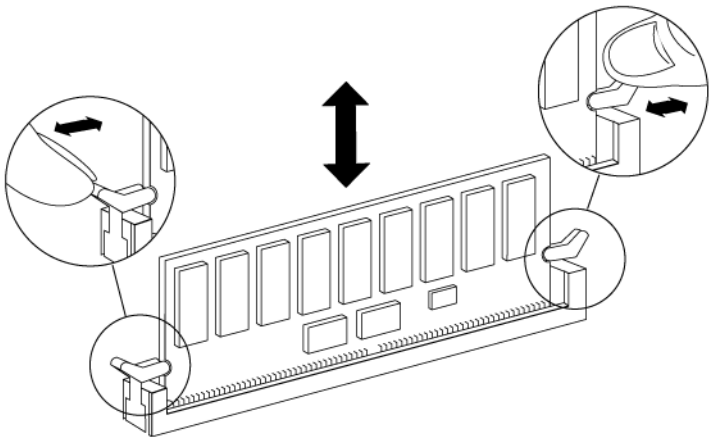
   If you are moving DIMMs on a FAS22xx system:



1	System DIMM
2	NVMEM DIMM The NVMEM DIMM has an *NVMEM* label on one of the chips.
3	NVMEM battery plug
4	System DIMM slot
5	NVMEM DIMM slot The NVMEM DIMM slot has white ejector tabs and is adjacent to the NVMEM battery.

3. Note the location and orientation of the DIMM in the socket so that you can insert it in the new controller module in the proper orientation.

4. Slowly press down on the two DIMM ejector tabs, one at a time, to eject the DIMM from its slot, and then lift it out of the slot.



Attention: You must carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

5. Locate the corresponding slot for the DIMM in the new controller module, align the DIMM over the slot, and then insert the DIMM into the slot.

   The notch among the pins on the DIMM should align with the tab in the socket. The DIMM fits tightly in the slot but should go in easily. If not, you should realign the DIMM with the slot and reinsert it.

   Important: You must install the NVMEM DIMM only in the NVMEM DIMM slot.

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

   The edge connector on the DIMM must make complete contact with the slot.

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

8. Repeat these steps to move additional DIMMs, as required.

9. In the new controller module, orient the NVMEM battery cable connector to the socket on the controller module and plug the cable into the socket.

   You must ensure that the plug locks down onto the socket on the controller module.

Installing the new controller module and booting the system

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

About this task

For HA pairs with two controller modules in the same chassis, the sequence in which you reinstall the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

Note: The system might update the system firmware when it boots. Do not abort this process.

Steps

1. Close and latch the controller module cover, if necessary.

2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Note: Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the management port so that you can access the system to perform the tasks in the following sections.
4. Complete the reinstall of the controller module:

If your system is in...	Then perform these steps...
An HA pair	**a.** With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. **Attention:** Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors. **b.** Enter one of the following commands from the healthy node's console and wait for the giveback to complete: For systems operating in... / Issue the command... 7-Mode / `cf giveback` Clustered Data ONTAP / • In Data ONTAP 8.2 or later: `storage failover giveback –ofnode impaired_node_name` **c.** If you have not already done so, reinstall the cable management , and then tighten the thumbscrew on the cam handle on back of the controller module. **d.** Bind the cables to the cable management device with the hook and loop strap.
A stand-alone configuration	**a.** With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. **Attention:** Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors. **b.** Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process. **c.** If you have not already done so, reinstall the cable management , and then tighten the thumbscrew on the cam handle on back of the controller module. **d.** Bind the cables to the cable management device with the hook and loop strap.

Important: During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must confirm that the healthy node remains down.

You can safely respond **Y** to these prompts.

Verifying and setting the HA state of the controller module

You must verify the **HA** state of the controller module and, if necessary, update the state to match your system configuration (HA pair or stand-alone).

Steps

1. In Maintenance mode, display the **HA** state of the new controller module and chassis:

   ha-config show

   The **HA** state should be the same for all components.

If your system is...	The HA state for all components should be...
In an HA pair	ha
Stand-alone	non-ha

2. If the displayed system state of the controller does not match your system configuration, set the **HA** state for the controller module:

   ha-config modify controller *ha-state*

If your system is...	Issue the following command...
In an HA pair	**ha-config modify controller ha**
Stand-alone	**ha-config modify controller non-ha**

3. If the displayed system state of the chassis does not match your system configuration, set the **HA** state for the chassis:

   ha-config modify chassis *ha-state*

If your system is...	Issue the following command...
In an HA pair	**ha-config modify chassis ha**
Stand-alone	**ha-config modify chassis non-ha**

Restoring Fibre Channel configurations

The onboard Fibre Channel (FC) ports are not preconfigured, you must restore any FC port configurations in your HA pair before you bring the node back into service; otherwise, you might experience a disruption in service. Systems without FC configurations can skip this procedure.

Before you begin

You must have the values of the FC port settings that you saved earlier.

Steps

1. From the healthy node, verify the values of the FC configuration on the replacement node: **partner fcadmin config**
2. Compare the default FC variable settings with the list you saved earlier.

If the FC variables are...	Then...
The same as you recorded earlier	Proceed to the next step in this procedure.

If the FC variables are...	Then...
Different than you recorded earlier	**a.** If you have not already done so, reboot the replacement node to Maintenance mode by pressing **Ctrl-C** when you see the message `Press Ctrl-C for Boot Menu`. **b.** Answer **y** when prompted by the system. **c.** Select the Maintenance mode option from the displayed menu. **d.** Enter one of the following commands, depending on what you need to do: • To program target ports: **fcadmin config -t target *adapter_name*** • To program initiator ports: **fcadmin config -t initiator *adapter_name*** • To unconfigure ports: **fcadmin config -t unconfigure *adapter_name*** **e.** Verify the values of the variables by entering the following command: **fcadmin config** **f.** Exit Maintenance mode by entering the following command: **halt** After you issue the command, wait until the system stops at the LOADER prompt.

Setting the system time after replacing the controller module

If your system is in an HA pair, you must set the time on the replacement node to that of the healthy node to prevent possible outages on clients due to time differences.

About this task

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

- The *replacement node* is the new node that replaced the impaired node as part of this procedure.
- The *healthy node* is the HA partner of the replacement node.

When setting the date and time at the LOADER prompt, verify that all times are set to GMT.

Steps

1. If you have not already done so, halt the replacement node to display the LOADER prompt.
2. Determine the system time by using the `date` command on the healthy node (if the system is in an HA pair) or another reliable time source.
3. Set the date in GMT on the replacement node:
   set date *mm/dd/yyyy*
4. Set the time in GMT on the replacement node:
   set time *hh*:*mm*:*ss*

Installing the firmware after replacing the controller module

After replacing the controller module, you must install the latest firmware if your system is running a version of Data ONTAP earlier than 8.2, and check and update the Service Processor (SP) firmware if needed, on the new controller module. If the

system is in an HA pair, the healthy node should also be updated so that each controller module is running the same firmware version.

About this task

If your system is running ONTAP 8.2 or later, the SP firmware and BIOS automatically update to the baseline image included with the ONTAP version. Other system firmware from the old controller module still resides on the boot device and typically does not need updating.

If your system is running ONTAP 8.2 or later, you should skip this procedure.

Steps

1. Check the configuration of the SP from the LOADER prompt:

   `sp status`

   For the latest release of SP firmware, log in to the NetApp Support Site at *mysupport.netapp.com* and update it, if needed, in the following steps.

2. Log in to the SP from an administration host:

   `ssh username@SP_IP_address`

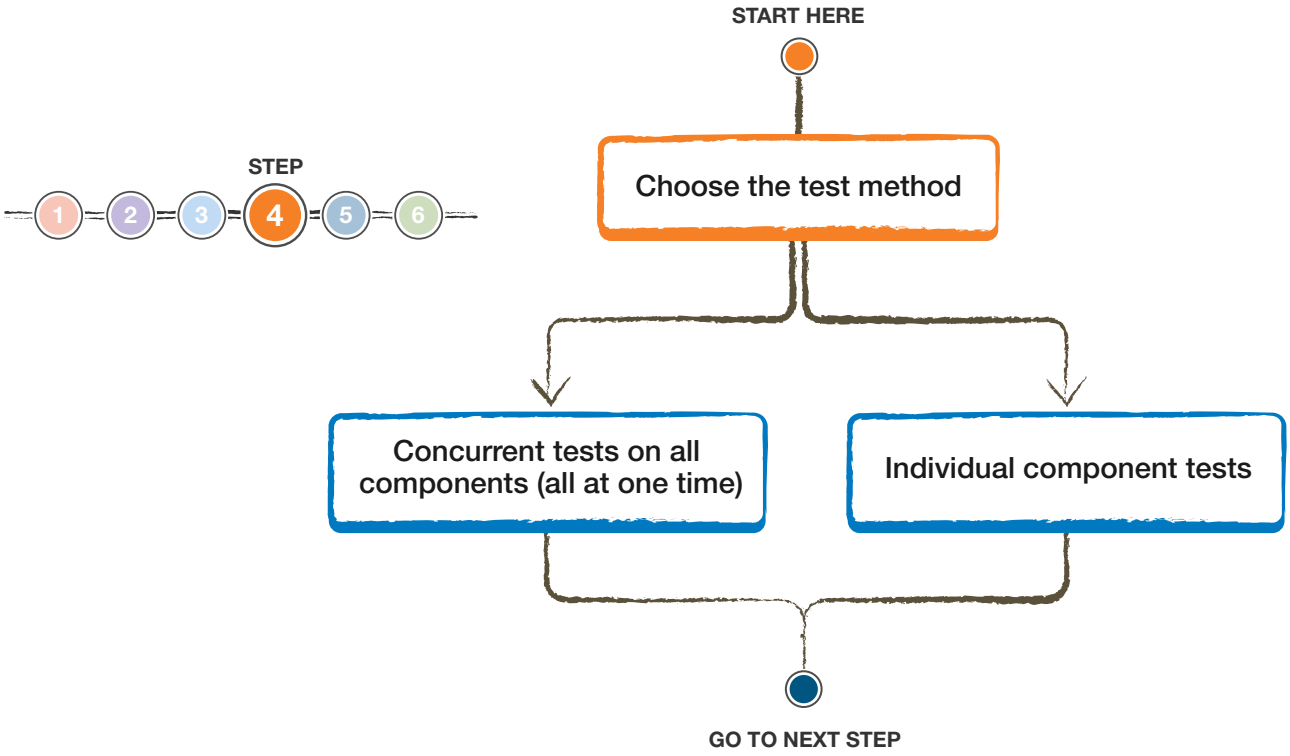
3. Download and install the most current version of firmware for your system by following the provided instructions.

   NetApp Downloads: System Firmware and Diagnostics

   Note: You can also take this opportunity to download and install the SP firmware and BIOS on the healthy node, if needed.

Running diagnostics tests after replacing a controller module

You should run focused diagnostic tests for specific components and subsystems whenever you replace a component of the controller.



Before you begin

- Your system must be at the LOADER prompt to start system-level diagnostics.
- For ONTAP 8.2 and later, you do not require loopback plugs to run tests on storage interfaces.

About this task

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, bring it to the LOADER prompt.
2. On the node with the replaced component, run the system-level diagnostic test: **`boot_diags`**

   Note: You must enter this command from the LOADER prompt for system-level diagnostics to function properly. The `boot_diags` command starts special drivers that are designed specifically for system-level diagnostics.

   Important: During the `boot_diags` process, you might see a prompt warning that when entering Maintenance mode in an HA configuration, you must confirm that the partner remains down.

   To continue to Maintenance mode, you should enter **`y`**

3. Clear the status logs: **`sldiag device clearstatus`**
4. Display and note the available devices on the controller module: **`sldiag device show -dev mb`**

   The controller module devices and ports that are displayed can be any one or more of the following:

- **bootmedia** is the system booting device.
- **env** is the motherboard environmentals.
- **mem** is the system memory.
- **nic** is a network interface card.
- **nvmem** is a hybrid of NVRAM and system memory.
- **sas** is a Serial Attached SCSI device that is not connected to a disk shelf.

5. How you proceed depends on how you want to run diagnostics on your system.

Choices

- Running diagnostics tests concurrently after replacing the controller module on page 18
- Running diagnostics tests individually after replacing the controller module on page 19

Running diagnostics tests concurrently after replacing the controller module

After replacing the controller module, you can run diagnostics tests concurrently if you want a single organized log of all the test results for all the devices.

About this task

The time required to complete this procedure can vary based on the choices that you make. If you run more tests in addition to the default tests, the diagnostic test process takes longer to complete.

Steps

1. Display and note the available devices on the controller module: **sldiag device show -dev mb**

   The controller module devices and ports that are displayed can be any one or more of the following:

   - **bootmedia** is the system booting device.
   - **env** is the motherboard environmentals.
   - **mem** is the system memory.
   - **nic** is a network interface card.
   - **nvmem** is a hybrid of NVRAM and system memory.
   - **sas** is a Serial Attached SCSI device that is not connected to a disk shelf.

2. Review the enabled and disabled devices in the output from step *1* on page 18 and then determine which tests you want to run concurrently.

3. List the individual tests for each device:

   sldiag device show -dev *dev_name*

4. Examine the output and, if applicable, enable the tests that you want to run for the device:

   sldiag device modify -dev *dev_name* -index *test_index_number* -selection enable

   test_index_number can be an individual number, a series of numbers separated by commas, or a range of numbers.

5. Examine the output and, if applicable, disable the tests that you do not want to run for the device by selecting only the tests that you want to run:

   sldiag device modify -dev *dev_name* -index *test_index_number* -selection disable

6. Verify that the tests were modified: **sldiag device show**
7. Repeat steps *2* on page 18 through *6* on page 18 for each device.
8. Run diagnostics on all the devices: **sldiag device run**

   Attention: You must not add to or modify your entries after you start running diagnostics.

   The tests are complete when the following message is displayed:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

9. After the tests are complete, verify that there are no hardware problems on your storage system:

   sldiag device status -long -state failed
10. Correct any issues that are found, and repeat this procedure.

Running diagnostics tests individually after replacing the controller module

After replacing the controller module, you can run diagnostics tests individually if you want a separate log of all the test results for each device.

Steps

1. Clear the status logs: **sldiag device clearstatus**
2. Display the available tests for the selected devices:

Device type	Command
boot media	**sldiag device show -dev bootmedia**
env	**sldiag device show -dev env**
mem	**sldiag device show -dev mem**
nic	**sldiag device show -dev nic**
nvmem	**sldiag device show -dev nvmem**
sas	**sldiag device show -dev sas**

3. Examine the output and, if applicable, enable the tests that you want to run for the device:

   sldiag device modify -dev *dev_name* -index *test_index_number* -selection enable

   test_index_number can be an individual number, a series of numbers separated by commas, or a range of numbers.
4. Examine the output and, if applicable, disable the tests that you do not want to run for the device by selecting only the tests that you want to run:

   sldiag device modify -dev *dev_name* -index *test_index_number* -selection only
5. Run the selected tests:

Device type	Command
boot media	**sldiag device run -dev bootmedia**
env	**sldiag device run -dev env**

Device type	Command
mem	**sldiag device run -dev mem**
nic	**sldiag device run -dev nic**
nvmem	**sldiag device run -dev nvmem**
sas	**sldiag device run -dev sas**

After the test is complete, the following message is displayed:

```
<SLDIAG:_ALL_TESTS_COMPLETED>
```

6. Verify that no tests failed:

Device type	Command
boot media	**sldiag device status -dev bootmedia -long -state failed**
env	**sldiag device status -dev env -long -state failed**
mem	**sldiag device status -dev mem -long -state failed**
nic	**sldiag device status -dev nic -long -state failed**
nvmem	**sldiag device status -dev nvmem**
sas	**sldiag device status -dev sas -long -state failed**

Any tests that failed are displayed.

7. Proceed based on the result of the preceding step:

If the system-level diagnostics tests...	Then...
Were completed without any failures	**a.** Clear the status logs: **sldiag device clearstatus** **b.** Verify that the log is cleared: **sldiag device status** The following default response is displayed: `SLDIAG: No log messages are present.` You have completed system-level diagnostics.

If the system-level diagnostics tests...	Then...
Resulted in some test failures	Determine the cause of the problem: **a.** Exit Maintenance mode: **`halt`** After you issue the command, wait until the system stops at the LOADER prompt. **b.** Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: • If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. • If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. **c.** Check the controller module you are servicing and verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. **d.** Boot the controller module you are servicing, interrupting the boot by pressing **`Ctrl-C`** when prompted. This takes you to the Boot menu: • If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. • If you have one controller module in the chassis, connect the power supplies and turn them on. **e.** Select Boot to Maintenance mode from the menu. **f.** Exit Maintenance mode: **`halt`** After you issue the command, you must wait until the system stops at the LOADER prompt. **g.** Enter **`boot_diags`** at the prompt and rerun the system-level diagnostic test.

8. Continue to the next device that you want to test, or exit system-level diagnostics and continue with the procedure.

Recabling the system

After running diagnostics, you must recable the storage and network connections of the controller module.

Steps

1. Reinstall the cable management arms and recable the controller module, as needed.
2. Check your cabling using Config Advisor.
   a. Download and install Config Advisor from the NetApp Support Site at *mysupport.netapp.com*
   b. Enter the information for the target system, and then click **Collect Data**.
   c. Click the **Cabling** tab, and examine the output.

      You must verify that all disk shelves are displayed and that all disks appear in the output. You must correct any cabling issues that you might find.
   d. Check other cabling by clicking the appropriate tab, and examining the output from Config Advisor.

Reassigning disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.

About this task

You must use the correct procedure for your configuration:

If the controller is in...	Then use this procedure...
An HA pair	*Verifying the system ID change on a system operating in 7-Mode* on page 22
A stand-alone configuration	*Manually reassigning the system ID on a stand-alone system in 7-mode* on page 23

Verifying the system ID change on an HA system operating in 7-Mode

You must confirm the system ID change when you boot the replacement node, and then verify that the change was implemented.

About this task

This procedure applies only to systems that are in an HA pair and are running Data ONTAP operating in 7-Mode.

Steps

1. If the replacement node is in Maintenance mode (showing the *> prompt), exit Maintenance mode:

   `halt`

   After you issue the command, you must wait until the system stops at the LOADER prompt.

2. From the LOADER prompt on the replacement node, display the Boot menu:

   a. Boot the replacement node:

      `boot_ontap`

   b. Press **`Ctrl-c`** when prompted to display the Boot menu.

3. Wait until the `Waiting for giveback...` message is displayed on the console of the replacement node and then, on the healthy node, verify that the controller module replacement has been detected and that the new partner system ID has been automatically assigned:

   `cf status`

   You should see a message similar to the following, which indicates that the system ID change has been detected:

   ```
   HA mode.
   System ID changed on partner (Old: 1873774576, New: 1873774574).
   partner_node has taken over target_node.
   target_node is ready for giveback.
   ```

   The message shows the new system ID of the replacement node. In this example, the new system ID is 1873774574.

4. From the healthy node, verify that all coredumps are saved: **`partner savecore`**

   If the command output indicates that savecore is in progress, you must wait for savecore to finish before initiating the giveback operation. You can monitor the progress of the savecore: **`partner savecore -s`**

5. Initiate the giveback operation after the replacement node displays the `Waiting for Giveback...` message:

`cf giveback`

You should see a message similar to the following noting the system ID change and prompting you to continue:

```
System ID changed on partner. Giveback will update the ownership of partner disks with
system ID: 1873774574.
Do you wish to continue {y|n}?
```

You must enter **`y`** to proceed. If the giveback is vetoed, you can consider overriding the veto.

Find the High-Availability Configuration Guide for your version of ONTAP 9

Find the High-Availability Configuration Guide for your version of Data ONTAP 8

Find the Active/Active Configuration Guide for your version of Data ONTAP 7G

6. Verify that the disks were assigned correctly:

   `disk show`

   You must verify that the disks belonging to the replacement node show the new system ID for the replacement node. In the following example, the disks owned by node2 now show the new system ID, 1873774574:

   Example

```
system-1> disk show
  DISK            OWNER         POOL   SERIAL NUMBER  HOME           DR HOME
--------------    ------------- -----  -------------  -------------  ------------------
disk_name node2    (1873774574) Pool0  J8Y0TDZC       system-2       (1873774574)
disk_name node1     (118065578) Pool0  J8Y09DXC       system-1        (118065578)
.
.
.
```

7. Verify that the expected volumes are present and are online for each node:

   `vol status`

Manually reassigning the system ID on a stand-alone system operating in 7-Mode

In a stand-alone system, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies to stand-alone systems that are operating in 7-Mode.

Steps

1. If you have not already done so, reboot the replacement node, interrupt the boot process by entering **`Ctrl-C`**, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter **`Y`** when prompted to override the system ID due to a system ID mismatch.

2. View the system IDs:

   `disk show -a`

   Note: Make a note of the old system ID, which is displayed as part of the disk owner column.

   Example

   The following example shows the old system ID of 118073209:

```
*> disk show -a
Local System ID: 118065481

 DISK     OWNER        POOL    SERIAL NUMBER   HOME
--------  -----------  ------  -------------   -------------
system-1  (118073209)  Pool0   J8XJE9LC        system-1  (118073209)
system-1  (118073209)  Pool0   J8Y478RC        system-1  (118073209)
.
.
.
```

3. Reassign disk ownership by using the system ID information obtained from the `disk show` command:

   `disk reassign -s old system ID`

   In the case of the preceding example, the command is: **`disk reassign -s 118073209`**

   You can respond **`Y`** when prompted to continue.

4. Verify that the disks were assigned correctly:

   `disk show -a`

   You must verify that the disks belonging to the replacement node show the new system ID for the replacement node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

   Example

```
*> disk show -a
Local System ID: 118065481

  DISK     OWNER          POOL   SERIAL NUMBER  HOME
-------    -------------  -----  -------------  -------------
system-1  (118065481)     Pool0  J8Y0TDZC       system-1  (118065481)
system-1  (118065481)     Pool0  J8Y09DXC       system-1  (118065481)
.
.
.
```

5. If the replacement node is in Maintenance mode (showing the *> prompt), exit Maintenance mode:

   `halt`

   After you issue the command, you must wait until the system stops at the LOADER prompt.

6. Boot the operating system:

   `boot_ontap`

Restoring Storage Encryption functionality after replacing controller modules

After replacing the controller module for a storage system that you previously configured to use Storage Encryption, you must perform additional steps to restore Storage Encryption functionality in an uninterrupted way. You can skip this task on storage systems that do not have Storage Encryption enabled.

Steps

1. Reconfigure Storage Encryption at the storage system prompt: **`key_manager setup`**
2. Complete the steps in the setup wizard to configure Storage Encryption.

   You must verify that a new passphrase is generated, and you must select **Yes** to lock all drives.

3. Repeat step *1* on page 24 and step *2* on page 24 on the partner node.

   You should not proceed to the next step until you have completed the Storage Encryption setup wizard on each node.

4. On each node, verify that all disks are rekeyed: **`disk encrypt show`**

   None of the disks should list a key ID of 0x0.

5. On each node, load all authentication keys: **`key_manager restore -all`**

6. On each node, verify that all keys are stored on their key management servers: **`key_manager query`**

   None of the key IDs should have an asterisk next to it.

Installing licenses for replacement nodes operating in 7-Mode

You must reinstall new license keys for replacement nodes for each feature package that was on the impaired node. The same license packages should be installed on both controller modules in an HA pair. Each controller module requires its own license keys.

About this task

Some features require that you enable certain options instead of, or in addition to, installing a license key. For detailed information about licensing, see knowledgebase article 3013749 at *NetApp KB Article 3013749: Data ONTAP 8.2 and 8.3 Licensing Overview and References* and the *Data ONTAP System Administration Guide for 7-Mode*.

The licenses keys must be in the 28-character format that is used by Data ONTAP 8.2.

You have a 90-day grace period to install the license keys; after the grace period, all old licenses are invalidated. Once a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

You can use the `license show` command to check the time available before the grace period expires.

Steps

1. If you require new license keys in the Data ONTAP 8.2 format, obtain replacement license keys on the NetApp Support Site in the **My Support** section under Software licenses.

   Note: The new license keys that you require are auto-generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. You must wait until the ONTAP command-line interface has been up for at least five minutes and then confirm that the license database is running.

3. Install the license keys:

   `license add *license_key license_key license_key...*`

   You can add one license or multiple licenses simultaneously, with each license key separated by a comma or a space.

   If the ONTAP command-line interface was not up for a sufficient amount of time, you might receive a message indicating that the license database is unavailable.

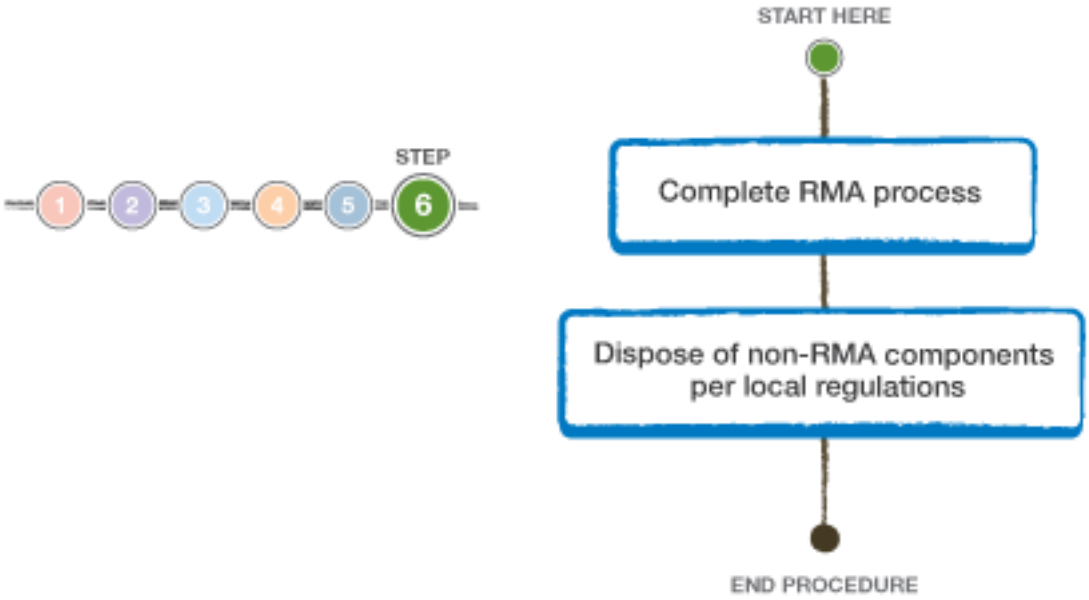
4. Verify that the licenses have been installed:

   `license show`

Completing the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at *NetApp Support*, 888-463-8277 (North America), 00-800-44-638277 (Europe), or

+800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.



Disposing of batteries

You must dispose of batteries according to the local regulations regarding battery recycling or disposal. If you cannot properly dispose of batteries, you must return the batteries to NetApp, as described in the RMA instructions that are shipped with the kit.

Related information

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Replacing a controller module in ONTAP

You must follow a specific series of steps to replace the depending on your mode and version of ONTAP.

Steps

1. Preparing for SAN configurations on page 27
2. Preparing for Storage Encryption configurations on page 27
3. Shutting down a node running ONTAP on page 28
4. Removing the controller module and moving the components on page 31
5. Installing the new controller and booting the system on page 38
6. Verifying and setting the HA state of the controller module on page 40
7. Restoring Fibre Channel configurations on page 41
8. Setting the system time after replacing the controller module on page 41
9. Installing the firmware after replacing the controller module on page 42
10. Running diagnostics tests after replacing a controller module on page 42
11. Recabling the system on page 47
12. Reassigning disks on page 48

13. Installing licenses for the replacement node in clustered Data ONTAP on page 53
14. Restoring Storage Encryption functionality after controller module replacement on page 54
15. Completing the replacement process on page 54

Preparing for SAN configurations

If you have a SAN configuration and the controller modules are in an HA pair, you must save the FC port configuration information before replacing the controller module so that you can reenter the information on the new controller module. You must also check whether the SCSI process is in quorum with the other nodes in the cluster.

Steps

1. Save the port configuration information for the impaired node:

If your system is running...	Then...
Data ONTAP 8.2.1 and earlier	Run the following command on the console of the healthy node: **`partner fcadmin config`** **Note:** If the impaired node is taken over by its partner, you can boot the impaired node to Maintenance mode, and then run the `fcadmin config` command in Maintenance mode.
ONTAP 8.2.2 and later	a. Run the following command on the console of the impaired node: **`system node hardware unified-connect show`** b. Run the following `Cluster-Mode` command on the console of the impaired node: **`system node hardware unified-connect modify`**

2. Copy and save the information displayed on the screen to a safe location for later reuse.

Preparing for Storage Encryption configurations

If the storage system whose controller you are replacing is configured to use Storage Encryption, you must first reset the authentication keys of the disks to an MSID key (the default security ID set by the manufacturer). This is a temporary necessity during the controller replacement process to avoid potential loss of access to the data.

About this task

After resetting the authentication keys to an MSID key, the data on the disks is no longer protected by secret authentication keys. You must verify the physical safety of the disks during the replacement or upgrade process.

Steps

1. Access the nodeshell:

   `system node run -node` ***`node_name`***

2. Display the key ID for each self-encrypting disk on the original system:

   `disk encrypt show`

Example

```
disk encrypt show
Disk       Key ID                                                           Locked?
0c.00.1    0x0                                                              No
0c.00.0    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.3    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.4    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.2    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.5    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
```

The first disk in the example is associated with an MSID key; the other disks are associated with a non-MSID key.

3. Examine the output of the `disk encrypt show` command, and if any disks are associated with a non-MSID key, rekey the disks to an MSID key by taking one of the following actions:

   - Rekey the disks individually, once for each disk:

     `disk encrypt rekey 0x0 disk_name`

   - Rekey all of the disks at once:

     `disk encrypt rekey 0x0 *`

4. Verify that all of the self-encrypting disks are associated with an MSID key:

   `disk encrypt show`

   #### Example

   The following example shows the output of the `disk encrypt show` command when all self-encrypting disks are associated with an MSID key:

```
cluster::> disk encrypt show
Disk       Key ID                                                           Locked?
---------- ---------------------------------------------------------------- -------
0b.10.23   0x0                                                              No
0b.10.18   0x0                                                              No
0b.10.0    0x0                                                              Yes
0b.10.12   0x0                                                              Yes
0b.10.3    0x0                                                              No
0b.10.15   0x0                                                              No
0a.00.1    0x0                                                              Yes
0a.00.2    0x0                                                              Yes
```

5. Exit the nodeshell and return to the clustershell:

   `exit`

6. Repeat step *1* on page 27 through step *5* on page 28 for each individual node or HA pair.

Shutting down a node running ONTAP

To shut down an impaired node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node storage.

About this task

You must leave the power supplies turned on at the end of this procedure to provide power to the healthy node.

Steps

1. If the system is running ONTAP, check the status of the nodes in the cluster:

   a. Change to the advanced privilege level:

      `set -privilege advanced`

   b. Identify where Epsilon resides on the cluster:

      `cluster show -epsilon *`

      similar to the following example:

```
Node         Health  Eligibility   Epsilon
------------ ------- ------------ ------------
node1        true    true          true
node2        true    true          false
```

```
node3        true    true          false
node4        true    true          false

4 entries were displayed.
```

Note: Epsilon must not be assigned to a node that has to be replaced.

Note: In a cluster with a single HA pair, Epsilon will not be assigned to either node.

c. Take one of the following actions, depending on the result of the command:

If...	Then...
All nodes show `true` for both health and eligibility and Epsilon is not assigned to the impaired node	**a.** Exit advanced mode: **`set -privilege admin`** **b.** Proceed to Step 3.
All nodes show `true` for both health and eligibility and Epsilon is assigned to the impaired node	**a.** Remove Epsilon from the node: **`cluster modify -node node1 -epsilon false`** **b.** Assign Epsilon to a node in the cluster: **`cluster modify -node node4 -epsilon true`** **c.** Exit advanced mode: **`set -privilege admin`** **d.** Go to Step 3.
The impaired node shows `false` for health and is the Epsilon node	**a.** Change to the advance privilege level: **`set -privilege advanced`** **b.** Remove Epsilon from the node: **`cluster modify -node node1 -epsilon false`** **c.** Assign Epsilon to a node in the cluster: **`cluster modify -node node4 -epsilon true`** **d.** Exit advanced mode: **`set -privilege admin`** **e.** Proceed to the next step.
The impaired node shows `false` for health and is not the Epsilon node	**a.** Proceed to the next step.
Any node shows `false` for eligibility	**a.** Resolve any cluster issues as needed . **b.** Exit advanced mode: **`set -privilege admin`**
Any node other than the impaired node shows `false` for health	**a.** Correct the problems that caused the health issues on the nodes. **b.** Exit advanced mode: **`set -privilege admin`**

2. If the impaired node is part of an HA pair, disable the `auto-giveback` option from the console of the healthy node:

   `storage failover modify -node local -auto-giveback false`

3. Bring the healthy node to the LOADER prompt:

If the impaired node is in...	Then...
A stand-alone configuration and is running	Halt the impaired node: **`system -node halt impaired_node_name`**
A stand-alone configuration and is not running and is not at the LOADER prompt	Resolve any issues that caused the node to quit running, power-cycle it, and then halt the boot process by entering **`Ctrl-C`** and responding **`Y`** to take the node to the LOADER prompt.
An HA pair	If the impaired node is at the LOADER prompt, it is ready for service. Otherwise, take one of the following actions, as applicable: • If the impaired node is showing the ONTAP prompt, take over the impaired node from the healthy node and be prepared to interrupt the reboot: **`storage failover takeover -ofnode impaired_node_name`** When prompted to interrupt the reboot, you must press **`Ctrl-C`** to go to the LOADER prompt. **Note:** In a two-node cluster, if Epsilon is assigned to the impaired node, you must move Epsilon to the healthy node before halting the impaired node. • If the display of the impaired node is showing the `Waiting for giveback` message, press **`Ctrl-C`** and respond **`Y`** to take the node to the LOADER prompt. • If the impaired node does not show either the `Waiting for giveback` message or an ONTAP prompt, power-cycle the node. You should contact technical support if the node does not respond to the power cycle.

4. Capture the Remote Service Agent (RSA) configuration:

   a. From the LOADER prompt, go to the Service Processor (SP) by entering **`^G`**.

   b. Enter the administrator password.

   c. Display the RSA settings:

      `rsa show`

   d. Exit the LOADER prompt:

      `exit`

5. Shut down the impaired node.

   Note: If the node is in an HA pair, the impaired node console should be showing the `Waiting for giveback...` message.

   The method that you use to shut down the node depends on whether remote management through the SP is used:

If the SP is...	Then...
Configured	Log in to the SP of the impaired node SP, and then turn off the power: **`system power off`** .
Not configured	At the impaired node prompt, press **`Ctrl-C`** and respond **`Y`** to halt the node.

6. If the system is in a stand-alone configuration, shut down the power supplies, and then unplug both of the power cords from the power source.

Removing the controller module and moving the components

You must remove the old controller module from the chassis and move all field-replaceable components from the old controller module to the new controller module.

About this task

Attention: If the system is in an HA pair, you must wait for two minutes after takeover of the impaired node to confirm that the takeover was successfully completed before removing the controller module.

To reduce the possibility of damage to the replaceable components, you should minimize handling by installing the components into the new controller module as soon as you remove them from the old controller module.

Steps

1. Removing the controller module from the system on page 31
2. Moving the mezzanine card on page 33
3. Moving the boot device on page 34
4. Moving the NVMEM battery on page 35
5. Moving the DIMMs to the new controller module on page 36

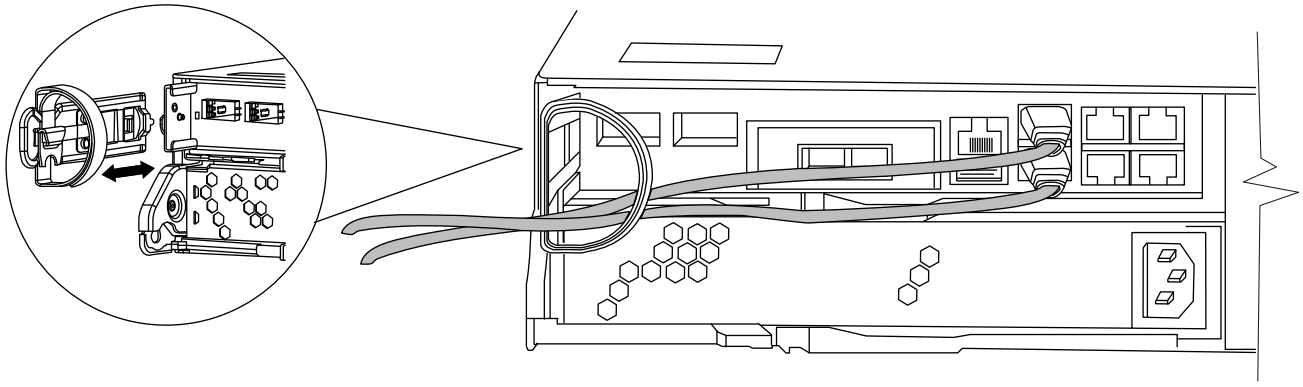
Removing the controller module from the system

To replace the controller module, you must first remove the old controller module from the system.

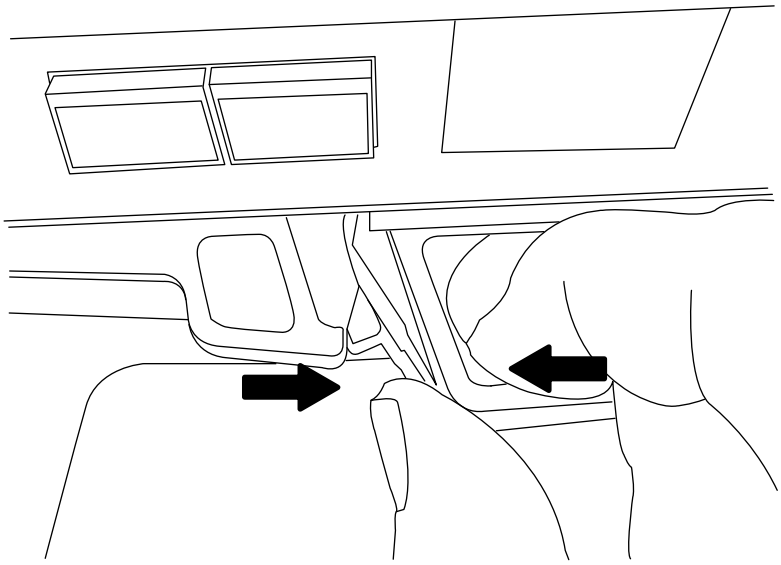
Steps

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management arm, and then unplug the system cables and SFPs (if needed) from the controller module, and keep track of where the cables were connected.

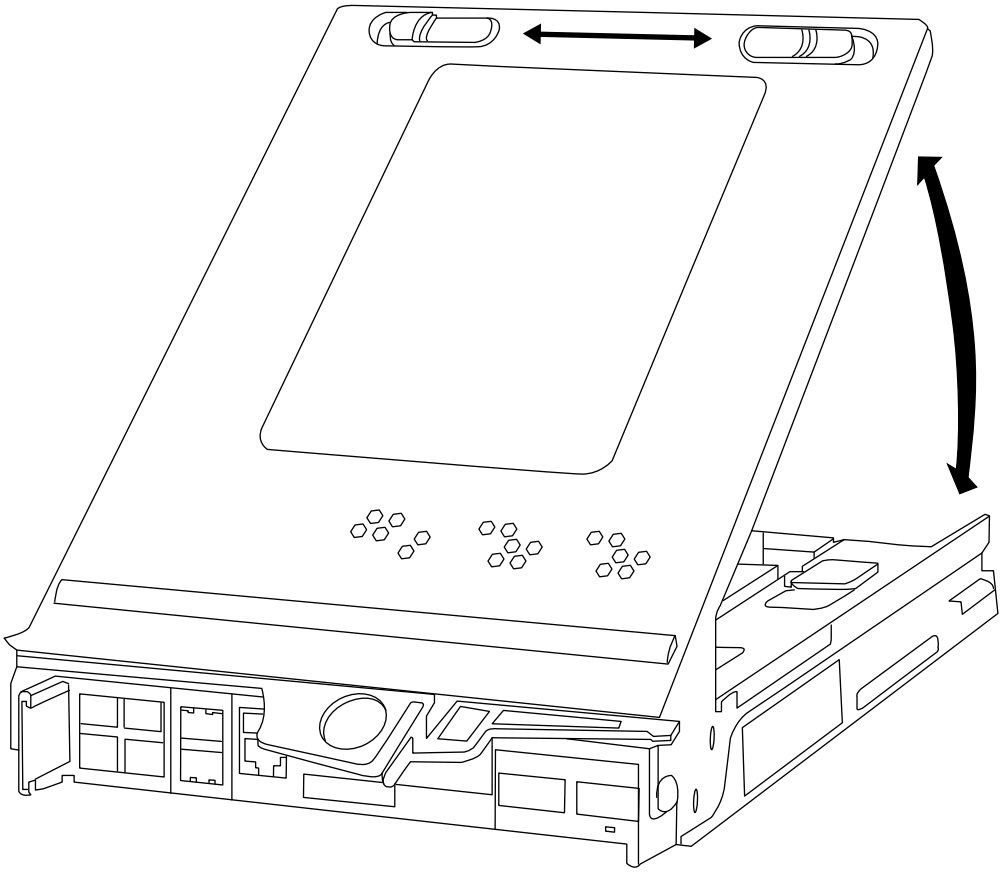
   Leave the cables in the cable management arm so that when you reinstall the cable management arm, the cables are organized.
3. Remove the cable management arms from the left and right sides of the controller module and set them aside.



   The illustration shows a FAS2220 or FAS2240-2 system. The procedure is the same for all FAS22xx systems.
4. Squeeze the latch on the cam handle until it releases, as shown in the following illustration. Open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and open it by sliding the blue tabs to release the cover, and then swing the cover up and open.

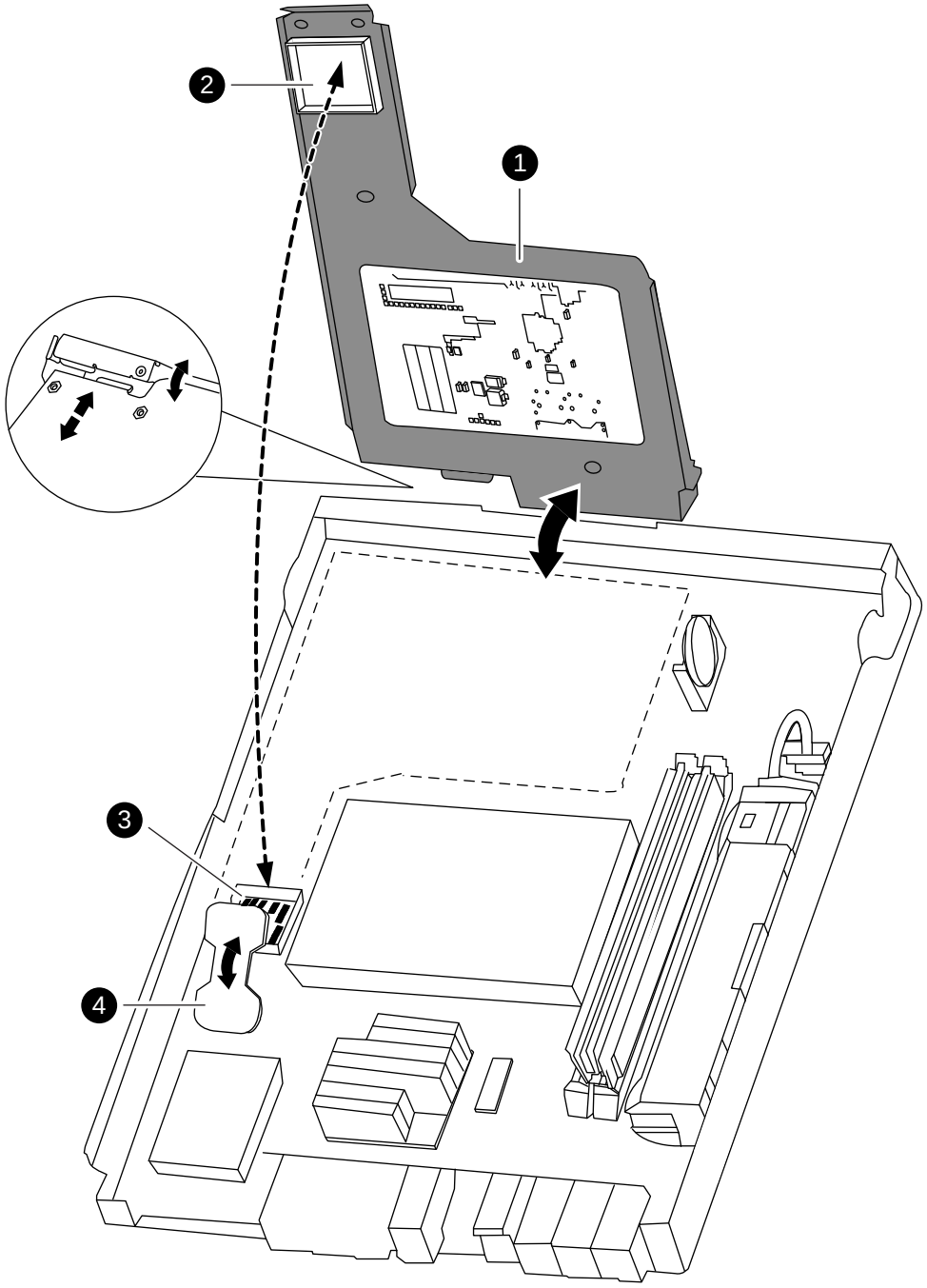


Moving the mezzanine card

If the system has a mezzanine card, you must move it from the old controller module to the new controller module to maintain airflow requirements or the selected I/O functionality.

Steps

1. Release the lever that holds the mezzanine blank or card in place.



1	Mezzanine card

2	Mezzanine card connector
3	Motherboard socket for mezzanine card connector
4	Lever (when closed, engages and locks the mezzanine card connector in the socket)

Note: The illustration shows a mezzanine card; the mezzanine blank does not have the circuit board.

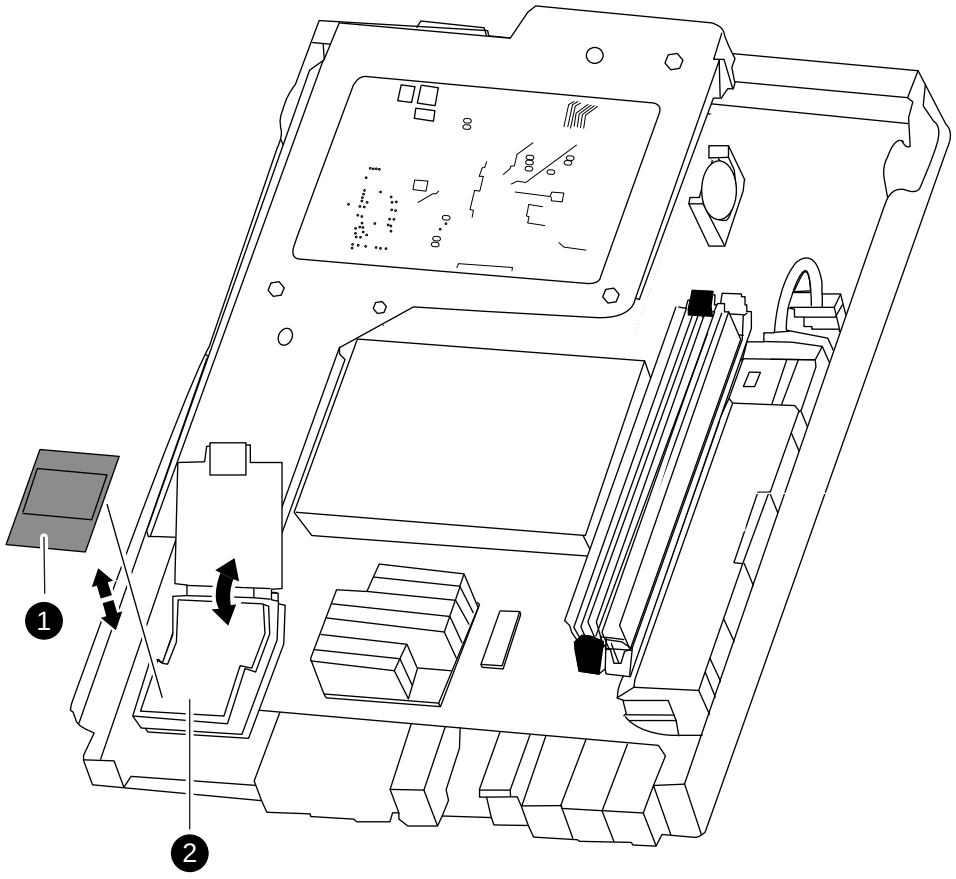
2. Swing the mezzanine blank or card up and lift it out of the controller module.
3. Align the mezzanine blank or card I/O panel in the slot in the front of the new controller module, and swing the mezzanine blank or card down to seat the connector into the socket on the controller module.
4. Close and push down on the blue lever to engage the mezzanine blank or card connector and to secure the mezzanine blank or card.

Moving the boot device

To move the boot device from the old controller module to the new controller module, you must perform a specific sequence of steps.

Steps

1. Locate the boot device using the following illustration or the FRU map on the controller module:



1	Boot device
2	Boot device holder; not removable

2. Open the boot device cover and hold the boot device by its edges at the notches in the boot device housing, gently lift it straight up and out of the housing.

   Attention: Always lift the boot device straight up out of the housing. Lifting it out at an angle can bend or break the connector pins in the boot device.

3. Open the boot device cover on the new controller module.
4. Align the boot device with the boot device socket or connector, and then firmly push the boot device straight down into the socket or connector.

   Important: Always install the boot device by aligning the front of the boot device squarely over the pins in the socket at the front of the boot device housing. Installing the boot device at an angle or over the rear plastic pin first can bend or damage the pins in the boot device connector.

5. Check the boot device to make sure that it is seated squarely and completely in the socket or connector.

   If necessary, remove the boot device and reseat it into the socket.

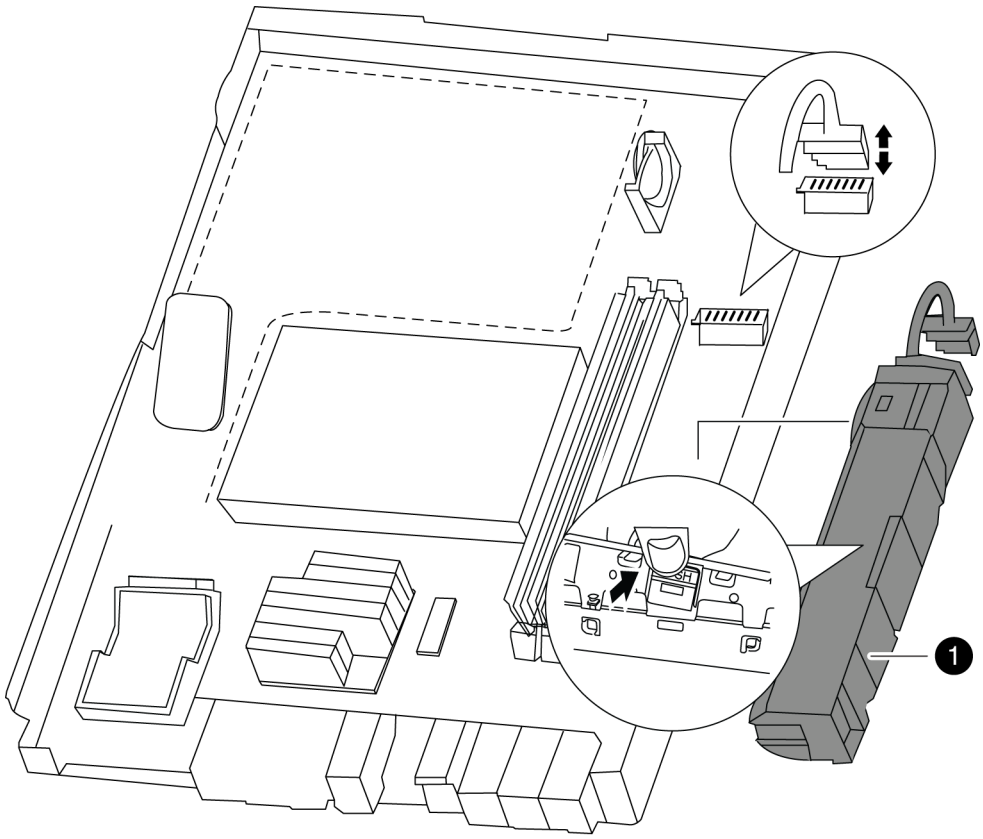
6. Close the boot device cover.

Moving the NVMEM battery

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

Steps

1. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.



1	NVMEM battery

2. Grasp the battery and press the tab marked PUSH, and then lift the battery out of the holder and controller module.
3. In the new controller module, seat the battery in the holder.

   Attention: Do not connect the NVMEM keyed battery plug into the socket until after the NVMEM DIMM has been installed.

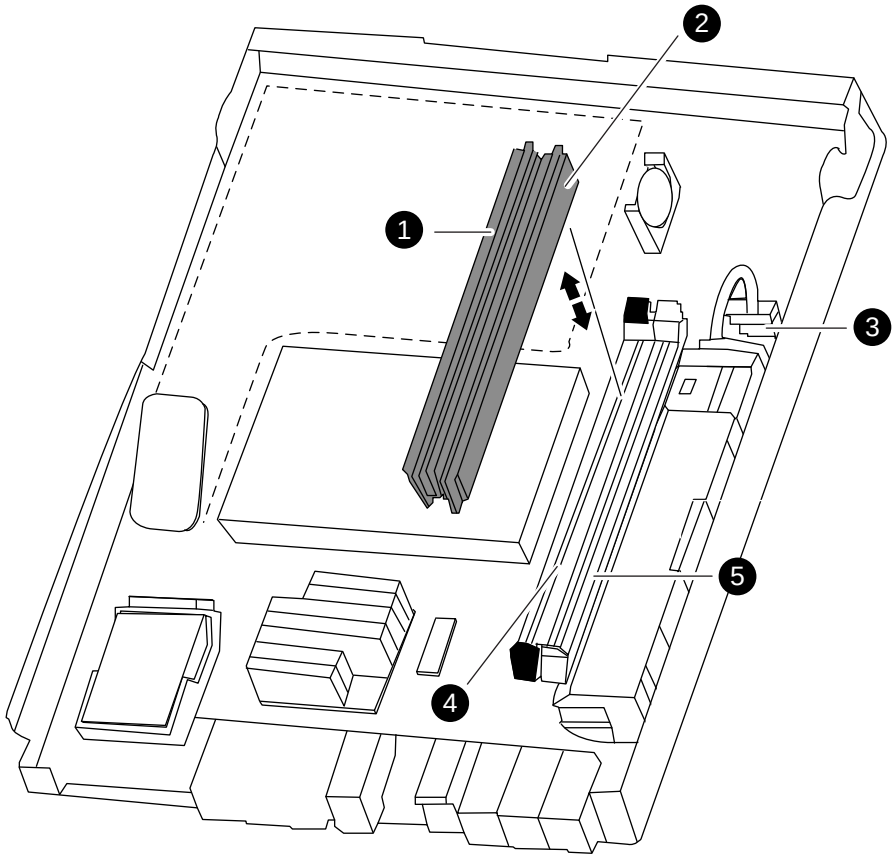
Moving the DIMMs to the new controller module

You must remove the DIMMs from the old controller module, being careful to note their locations so that you can reinstall them in the correct sockets in the new controller module.

Steps

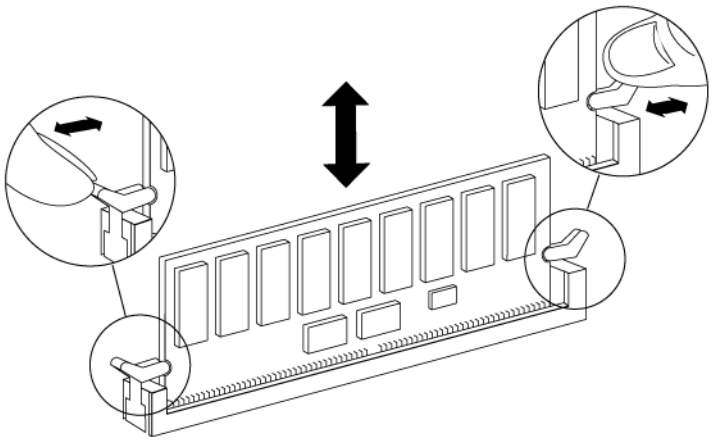
1. Verify that the NVMEM battery cable connector is not plugged into the socket .
2. Locate the DIMMs.

   If you are moving DIMMs on a FAS22xx system:



1	System DIMM
2	NVMEM DIMM The NVMEM DIMM has an *NVMEM* label on one of the chips.
3	NVMEM battery plug
4	System DIMM slot
5	NVMEM DIMM slot The NVMEM DIMM slot has white ejector tabs and is adjacent to the NVMEM battery.

3. Note the location and orientation of the DIMM in the socket so that you can insert it in the new controller module in the proper orientation.
4. Slowly press down on the two DIMM ejector tabs, one at a time, to eject the DIMM from its slot, and then lift it out of the slot.



Attention: You must carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

5. Locate the corresponding slot for the DIMM in the new controller module, align the DIMM over the slot, and then insert the DIMM into the slot.

   The notch among the pins on the DIMM should align with the tab in the socket. The DIMM fits tightly in the slot but should go in easily. If not, you should realign the DIMM with the slot and reinsert it.

   Important: You must install the NVMEM DIMM only in the NVMEM DIMM slot.

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

   The edge connector on the DIMM must make complete contact with the slot.

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

8. Repeat these steps to move additional DIMMs, as required.

9. In the new controller module, orient the NVMEM battery cable connector to the socket on the controller module and plug the cable into the socket.

   You must ensure that the plug locks down onto the socket on the controller module.

Installing the new controller and booting the system

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system.

Installing the new controller and booting in Data ONTAP 8.2.2 and later

After you install the components from the old controller module into the new controller module, you must install the new controller module into the system chassis and boot the operating system. How you complete this task depends on whether your system is a stand-alone system or part of an HA pair

About this task

Attention: For HA pairs with two controller modules in the same chassis, the sequence in which you reinstall the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

Your system configuration determines how you proceed:

- If you have two controller modules in the same chassis, complete the steps for an HA configuration.
- If you have one controller module in a stand-alone configuration, complete the steps for a stand-alone configuration.

Installing the controller and booting the system with two controller modules in the chassis

When you install the new controller module, you must follow a specific series of steps to prepare it for later tasks.

Steps

1. Close and latch the controller module cover, if necessary.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Note: Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the console port, but do not cable the Management port.
4. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

   Attention: Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.

5. Boot to the LOADER prompt by pressing **`Ctrl-C`** when you see the message `Press Ctrl-C for Boot Menu`.

   Note: If you miss the prompt, the system will reboot and give you another opportunity to boot to LOADER prompt.

   Important: During the boot process, you might see the following prompts:

   - A prompt warning of a system ID mismatch and a request to override the system ID
   - A prompt warning that when entering Maintenance mode in a HA configuration you must ensure that the healthy node remains down

   You can safely respond **`Y`** to these prompts.

6. Boot to maintenance mode by entering **`boot_ontap maint`** at the LOADER prompt.
7. Recable the Management port.
8. If you have not already done so, reinstall the cable management , and then tighten the thumbscrew on the cam handle on back of the controller module.
9. Bind the cables to the cable management device with the hook and loop strap.
10. Go to *Verifying and setting the HA state of the controller (after controller replacement)* on page 14.

Installing the controller and booting the system with one controller module in the chassis

Installing the controller module and booting the system is the same whether the system is a stand-alone system with one controller module in the chassis, or is an HA configuration with one controller module in each chassis.

Steps

1. Close and latch the controller module cover, if necessary.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Note: Do not completely insert the controller module in the chassis until instructed to do so.

3. Recable the console port, but do not cable the Management port.

4. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

   Attention: Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.

5. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process.

6. Boot to the LOADER prompt by pressing **Ctrl-C** when you see the message `Press Ctrl-C for Boot Menu`.

   Note: If you miss the prompt, the system will reboot and give you another opportunity to boot to LOADER prompt.

   Important: During the boot process, you might see the following prompts:

   - A prompt warning of a system ID mismatch and a request to override the system ID
   - A prompt warning that when entering Maintenance mode in a HA configuration you must ensure that the healthy node remains down

   You can safely respond **Y** to these prompts.

7. Boot to maintenance mode by entering **boot_ontap maint** at the LOADER prompt.

8. Recable the Management port.

9. If you have not already done so, reinstall the cable management , and then tighten the thumbscrew on the cam handle on back of the controller module.

10. Bind the cables to the cable management device with the hook and loop strap.

11. Go to *Verifying and setting the HA state of the controller (after controller replacement)* on page 14.

Verifying and setting the HA state of the controller module

You must verify the **HA** state of the controller module and, if necessary, update the state to match your system configuration (HA pair or stand-alone).

Steps

1. In Maintenance mode, display the **HA** state of the new controller module and chassis:

   ha-config show

   The **HA** state should be the same for all components.

If your system is...	The HA state for all components should be...
In an HA pair	`ha`
Stand-alone	`non-ha`

2. If the displayed system state of the controller does not match your system configuration, set the **HA** state for the controller module:

   ha-config modify controller *ha-state*

If your system is...	Issue the following command...
In an HA pair	**ha-config modify controller ha**
Stand-alone	**ha-config modify controller non-ha**

3. If the displayed system state of the chassis does not match your system configuration, set the **HA** state for the chassis:

ha-config modify chassis *ha-state*

If your system is...	Issue the following command...
In an HA pair	**ha-config modify chassis ha**
Stand-alone	**ha-config modify chassis non-ha**

Restoring Fibre Channel configurations

The onboard Fibre Channel (FC) ports are not preconfigured, you must restore any FC port configurations in your HA pair before you bring the node back into service; otherwise, you might experience a disruption in service. Systems without FC configurations can skip this procedure.

Before you begin

You must have the values of the FC port settings that you saved earlier.

Steps

1. From the healthy node, verify the values of the FC configuration on the replacement node:

   system node run -node *healthy-node-name* partner fcadmin config

2. Compare the default FC variable settings with the list you saved earlier.

If the FC variables are...	Then...
The same as you recorded earlier	Proceed to the next step in this procedure.
Different than you recorded earlier	**a.** If you have not already done so, reboot the replacement node to Maintenance mode by pressing **Ctrl-C** when you see the message `Press Ctrl-C for Boot Menu`. **b.** Answer **y** when prompted by the system. **c.** Select the Maintenance mode option from the displayed menu. **d.** Enter one of the following commands, depending on what you need to do: • To program target ports: **fcadmin config -t target *adapter_name*** • To program initiator ports: **fcadmin config -t initiator *adapter_name*** • To unconfigure ports: **fcadmin config -t unconfigure *adapter_name*** **e.** Verify the values of the variables by entering the following command: **fcadmin config**

Setting the system time after replacing the controller module

If your system is in an HA pair, you must set the time on the replacement node to that of the healthy node to prevent possible outages on clients due to time differences.

About this task

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

- The *replacement node* is the new node that replaced the impaired node as part of this procedure.

- The *healthy node* is the HA partner of the replacement node.

When setting the date and time at the LOADER prompt, verify that all times are set to GMT.

Steps

1. If you have not already done so, halt the replacement node to display the LOADER prompt.
2. Determine the system time by using the `date` command on the healthy node (if the system is in an HA pair) or another reliable time source.
3. Set the date in GMT on the replacement node:

   `set date mm/dd/yyyy`
4. Set the time in GMT on the replacement node:

   `set time hh:mm:ss`

Installing the firmware after replacing the controller module

After replacing the controller module, you must install the latest firmware if your system is running a version of Data ONTAP earlier than 8.2, and check and update the Service Processor (SP) firmware if needed, on the new controller module. If the system is in an HA pair, the healthy node should also be updated so that each controller module is running the same firmware version.

About this task

If your system is running ONTAP 8.2 or later, the SP firmware and BIOS automatically update to the baseline image included with the ONTAP version. Other system firmware from the old controller module still resides on the boot device and typically does not need updating.

If your system is running ONTAP 8.2 or later, you should skip this procedure.

Steps

1. Check the configuration of the SP from the LOADER prompt:

   `sp status`

   For the latest release of SP firmware, log in to the NetApp Support Site at *mysupport.netapp.com* and update it, if needed, in the following steps.
2. Log in to the SP from an administration host:

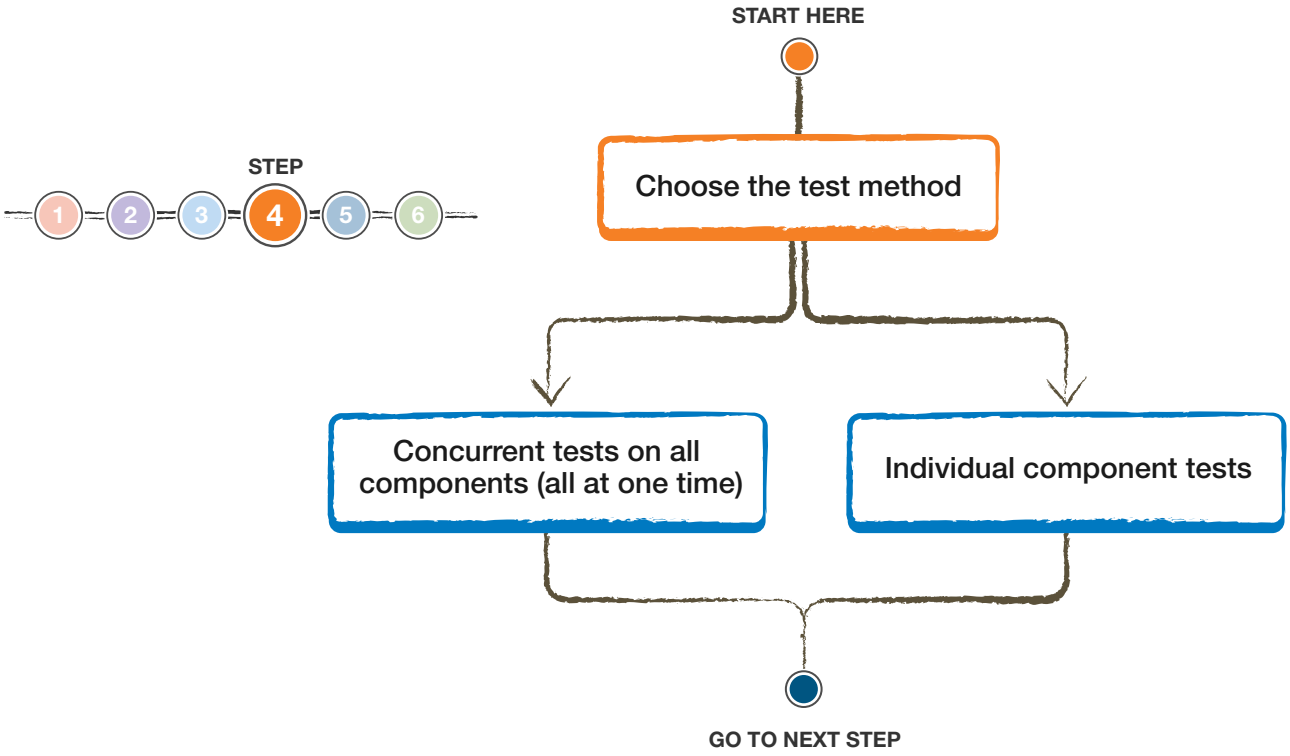
   `ssh username@SP_IP_address`
3. Download and install the most current version of firmware for your system by following the provided instructions.

   NetApp Downloads: System Firmware and Diagnostics

   Note: You can also take this opportunity to download and install the SP firmware and BIOS on the healthy node, if needed.

Running diagnostics tests after replacing a controller module

You should run focused diagnostic tests for specific components and subsystems whenever you replace a component of the controller.



Before you begin

- Your system must be at the LOADER prompt to start system-level diagnostics.
- For ONTAP 8.2 and later, you do not require loopback plugs to run tests on storage interfaces.

About this task

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

Steps

1. If the node to be serviced is not at the LOADER prompt, bring it to the LOADER prompt.
2. On the node with the replaced component, run the system-level diagnostic test: **`boot_diags`**

   Note: You must enter this command from the LOADER prompt for system-level diagnostics to function properly. The `boot_diags` command starts special drivers that are designed specifically for system-level diagnostics.

   Important: During the `boot_diags` process, you might see a prompt warning that when entering Maintenance mode in an HA configuration, you must confirm that the partner remains down.

   To continue to Maintenance mode, you should enter **`y`**

3. Clear the status logs: **`sldiag device clearstatus`**
4. Display and note the available devices on the controller module: **`sldiag device show -dev mb`**

   The controller module devices and ports that are displayed can be any one or more of the following:

- **bootmedia** is the system booting device.
- **env** is the motherboard environmentals.
- **mem** is the system memory.
- **nic** is a network interface card.
- **nvmem** is a hybrid of NVRAM and system memory.
- **sas** is a Serial Attached SCSI device that is not connected to a disk shelf.

5. How you proceed depends on how you want to run diagnostics on your system.

Choices

- Running diagnostics tests concurrently after replacing the controller module on page 44
- Running diagnostics tests individually after replacing the controller module on page 45

Running diagnostics tests concurrently after replacing the controller module

After replacing the controller module, you can run diagnostics tests concurrently if you want a single organized log of all the test results for all the devices.

About this task

The time required to complete this procedure can vary based on the choices that you make. If you run more tests in addition to the default tests, the diagnostic test process takes longer to complete.

Steps

1. Display and note the available devices on the controller module: **sldiag device show -dev mb**

   The controller module devices and ports that are displayed can be any one or more of the following:

   - **bootmedia** is the system booting device.
   - **env** is the motherboard environmentals.
   - **mem** is the system memory.
   - **nic** is a network interface card.
   - **nvmem** is a hybrid of NVRAM and system memory.
   - **sas** is a Serial Attached SCSI device that is not connected to a disk shelf.

2. Review the enabled and disabled devices in the output from step *1* on page 44 and then determine which tests you want to run concurrently.

3. List the individual tests for each device:

   sldiag device show -dev *dev_name*

4. Examine the output and, if applicable, enable the tests that you want to run for the device:

   sldiag device modify -dev *dev_name* -index *test_index_number* -selection enable

   test_index_number can be an individual number, a series of numbers separated by commas, or a range of numbers.

5. Examine the output and, if applicable, disable the tests that you do not want to run for the device by selecting only the tests that you want to run:

   sldiag device modify -dev *dev_name* -index *test_index_number* -selection disable

6. Verify that the tests were modified: **`sldiag device show`**
7. Repeat steps *2* on page 44 through *6* on page 44 for each device.
8. Run diagnostics on all the devices: **`sldiag device run`**

   Attention: You must not add to or modify your entries after you start running diagnostics.

   The tests are complete when the following message is displayed:

   ```
   *> <SLDIAG:_ALL_TESTS_COMPLETED>
   ```

9. After the tests are complete, verify that there are no hardware problems on your storage system:

   `sldiag device status -long -state failed`
10. Correct any issues that are found, and repeat this procedure.

Running diagnostics tests individually after replacing the controller module

After replacing the controller module, you can run diagnostics tests individually if you want a separate log of all the test results for each device.

Steps

1. Clear the status logs: **`sldiag device clearstatus`**
2. Display the available tests for the selected devices:

Device type	Command
`boot media`	**`sldiag device show -dev bootmedia`**
`env`	**`sldiag device show -dev env`**
`mem`	**`sldiag device show -dev mem`**
`nic`	**`sldiag device show -dev nic`**
`nvmem`	**`sldiag device show -dev nvmem`**
`sas`	**`sldiag device show -dev sas`**

3. Examine the output and, if applicable, enable the tests that you want to run for the device:

   `sldiag device modify -dev` ***`dev_name`*** **`-index`** ***`test_index_number`*** **`-selection enable`**

   `test_index_number` can be an individual number, a series of numbers separated by commas, or a range of numbers.
4. Examine the output and, if applicable, disable the tests that you do not want to run for the device by selecting only the tests that you want to run:

   `sldiag device modify -dev` ***`dev_name`*** **`-index`** ***`test_index_number`*** **`-selection only`**
5. Run the selected tests:

Device type	Command
`boot media`	**`sldiag device run -dev bootmedia`**
`env`	**`sldiag device run -dev env`**

Device type	Command
mem	**sldiag device run -dev mem**
nic	**sldiag device run -dev nic**
nvmem	**sldiag device run -dev nvmem**
sas	**sldiag device run -dev sas**

After the test is complete, the following message is displayed:

```
<SLDIAG:_ALL_TESTS_COMPLETED>
```

6. Verify that no tests failed:

Device type	Command
boot media	**sldiag device status -dev bootmedia -long -state failed**
env	**sldiag device status -dev env -long -state failed**
mem	**sldiag device status -dev mem -long -state failed**
nic	**sldiag device status -dev nic -long -state failed**
nvmem	**sldiag device status -dev nvmem**
sas	**sldiag device status -dev sas -long -state failed**

Any tests that failed are displayed.

7. Proceed based on the result of the preceding step:

If the system-level diagnostics tests...	Then...
Were completed without any failures	**a.** Clear the status logs: **sldiag device clearstatus** **b.** Verify that the log is cleared: **sldiag device status** The following default response is displayed: `SLDIAG: No log messages are present.` You have completed system-level diagnostics.

If the system-level diagnostics tests...	Then...
Resulted in some test failures	Determine the cause of the problem: **a.** Exit Maintenance mode: **`halt`** After you issue the command, wait until the system stops at the LOADER prompt. **b.** Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: • If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. • If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. **c.** Check the controller module you are servicing and verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. **d.** Boot the controller module you are servicing, interrupting the boot by pressing **`Ctrl-C`** when prompted. This takes you to the Boot menu: • If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis. The controller module boots up when fully seated. • If you have one controller module in the chassis, connect the power supplies and turn them on. **e.** Select Boot to Maintenance mode from the menu. **f.** Exit Maintenance mode: **`halt`** After you issue the command, you must wait until the system stops at the LOADER prompt. **g.** Enter **`boot_diags`** at the prompt and rerun the system-level diagnostic test.

8. Continue to the next device that you want to test, or exit system-level diagnostics and continue with the procedure.

Recabling the system

After running diagnostics, you must recable the storage and network connections of the controller module.

Steps

1. Reinstall the cable management arms and recable the controller module, as needed.
2. Check your cabling using Config Advisor.
   a. Download and install Config Advisor from the NetApp Support Site at *mysupport.netapp.com*
   b. Enter the information for the target system, and then click **Collect Data**.
   c. Click the **Cabling** tab, and examine the output.

      You must verify that all disk shelves are displayed and that all disks appear in the output. You must correct any cabling issues that you might find.
   d. Check other cabling by clicking the appropriate tab, and examining the output from Config Advisor.

Reassigning disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.

About this task

You must use the correct procedure for your configuration:

Controller redundancy	Then use this procedure...
HA pair	*Verifying the system ID change on a system operating in clustered Data ONTAP* on page 48
Stand-alone	*Manually reassigning the system ID on a stand-alone system in clustered Data ONTAP* on page 52

Verifying the system ID change on an HA system running clustered Data ONTAP

If you are running ONTAP 8.2 or later, you must confirm the system ID change when you boot the replacement node and then verify that the change was implemented.

About this task

This procedure applies only to systems running clustered Data ONTAP in an HA pair.

Steps

1. If the replacement node is in Maintenance mode (showing the *> prompt), exit Maintenance mode:

   `halt`

   After you issue the command, you must wait until the system stops at the LOADER prompt.

2. If you are running Data ONTAP 8.2.2 or earlier, on the replacement node at the prompt, confirm that the new controller module boots in clustered Data ONTAP:

   `setenv bootarg.init.boot_clustered true`

3. From the LOADER on the replacement node, boot the node

If you are running ONTAP...	Complete the following steps...
8.2.x and earlier	**a.** Boot the node: **`boot_ontap`** **b.** Press **`Ctrl-c`** when prompted to display the boot menu.
8.3 and later	Boot the node: **`boot_ontap menu`**

   If you are prompted to override the system ID due to a system ID mismatch, enter **`y`**.

4. Wait until the `Waiting for giveback...` message is displayed on the replacement node console and then, on the healthy node, verify that the controller module replacement has been detected and the new partner system ID has been automatically assigned.

Example

```
node1::*> storage failover show
                                 Takeover
Node              Partner        Possible     State Description
------------      ------------   --------     -----------------------------------
node1             node2          false        System ID changed on partner (Old:
                                               151759755, New: 151759706), In
takeover
node2             node1          -            Waiting for giveback (HA mailboxes)
```

5. From the healthy node, verify that any coredumps are saved:

   a. Change to the advanced privilege level:

      set -privilege advanced

      You can respond **Y** when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Save any coredumps:

      system node run -node *local-node-name* partner savecore

   c. Wait for savecore command to complete before issuing the giveback.

      You can enter the following command to monitor the progress of the savecore command:

      system node run -node *local-node-name* partner savecore -s

   d. Return to the admin privilege level:

      set -privilege admin

6. Your next step depends on the version of ONTAP your system is running.

If your system is running ...	Then...
Data ONTAP 8.2.0 and earlier or ONTAP 8.2.2 and later	Go to the next step.
Data ONTAP 8.2.1	Disable automatic takeover on reboot from the healthy node: **storage failover modify -node *replacement-node-name* -onreboot false**

7. Your next step depends on your version of ONTAP:

If your system is running...	Then...
Data ONTAP 8.2.0 and earlier or ONTAP 8.2.2 and later	Complete the following substeps after the replacement node is displaying the `Waiting for Giveback...` message: **a.** Give back the node: **`storage failover giveback -ofnode replacement_node_name`** As the replacement node boots up, it might again display the prompt warning of a system ID mismatch and asking to override the system ID. You can respond **`Y`**. The replacement node takes back its storage and completes booting up, and then reboots and id again taken over by the healthy node. As the replacement node boots up the second time, it might again display the prompt warning of a system ID mismatch and asking to override the system ID. You can respond **`Y`**. **b.** Once the node displays *`Waiting for Giveback...`*, give back the node: **`storage failover giveback -ofnode replacement_node_name`** As the replacement node boots up, it might again display the prompt warning of a system ID mismatch and asking to override the system ID. You can respond **`Y`**. The replacement node takes back its storage and completes booting up to the ONTAP prompt. **Note:** If the giveback is vetoed, you can consider overriding the vetoes. *ONTAP 9 High-Availability Configuration Guide* **c.** Monitor the progress of the giveback operation: `storage failover show-giveback` **d.** Wait until the `storage failover show-giveback` command output indicates that the giveback operation is complete. **e.** Confirm that the HA pair is healthy and takeover is possible: `storage failover show` The output from the `storage failover show` command should not include the "System ID changed on partner" message.

If your system is running...	Then...
Data ONTAP 8.2.1 only	Complete the following substeps after the replacement node is displaying the `Waiting for Giveback...` message: **a.** Give back the node: **`storage failover giveback -ofnode`** ***`replacement_node_name`*** As the replacement node boots up, it might display the prompt warning of a system ID mismatch and asking to override the system ID. You can respond **`Y`**. The replacement node takes back its storage, completes booting up and then reboots. **b.** Manually takeover the replacement node: **`storage failover takeover -ofnode`** ***`replacement_node_name`*** As the replacement node boots up the second time, it might again display the prompt warning of a system ID mismatch and asking to override the system ID. You can respond **`Y`**. **c.** Give back the node: **`storage failover giveback -ofnode`** ***`replacement_node_name`*** As the replacement node boots up, it might again display the prompt warning of a system ID mismatch and asking to override the system ID. You can respond y. The replacement node takes back its storage and completes booting up to the Data ONTAP prompt. **Note:** If the giveback is vetoed, you can consider overriding the vetoes. *ONTAP 9 High-Availability Configuration Guide* **d.** Monitor the progress of the giveback operation: `storage failover show-giveback` **e.** Wait until the `storage failover show-giveback` command output indicates that the giveback operation is complete. **f.** Confirm that the HA pair is healthy and takeover is possible: `storage failover show` The output from the `storage failover show` command should not include the "System ID changed on partner" message.

8. Verify that the disks or FlexArray Virtualization LUNS were assigned correctly:

   `storage disk show -ownership`

   Example

   Verify that the disks belonging to the replacement node should show the new system ID for the replacement node. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> storage disk show -ownership

Disk  Aggregate Home  Owner  DR Home  Home ID    Owner ID  DR Home ID Reserver  Pool
----- ------    ----- ------ -------- -------    -------    -------  ---------  ---
1.0.0  aggr0_1  node1 node1  -        1873775277 1873775277  -       1873775277 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -       1873775277 Pool0
.
.
.
```

9. Verify that the expected volumes are present for each node:

   `vol show -node` ***`node-name`***

10. If you disabled automatic takeover on reboot, reenable it on the healthy node console:

    storage failover modify -node *replacement-node-name* -onreboot true

Manually reassigning the system ID on a stand-alone system in clustered Data ONTAP

In a stand-alone system, you must manually reassign disks to the new controller's system ID and set the bootarg.init.boot_clustered bootarg before you return the system to normal operating condition.

About this task

This procedure applies only to systems that are running Data ONTAP operating in 7-Mode or are stand-alone.

Steps

1. If you have not already done so, reboot the replacement node, interrupt the boot process by entering **Ctrl-C**, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter **Y** when prompted to override the system ID due to a system ID mismatch.

2. View the system IDs:

   disk show -a

   Note: Make a note of the old system ID, which is displayed as part of the disk owner column.

   #### Example

   The following example shows the old system ID of 118073209:

   ```
   *> disk show -a
   Local System ID: 118065481

    DISK     OWNER        POOL    SERIAL NUMBER   HOME
   --------  -----------  ------  -------------   -------------
   system-1  (118073209)  Pool0   J8XJE9LC        system-1  (118073209)
   system-1  (118073209)  Pool0   J8Y478RC        system-1  (118073209)
   .
   .
   .
   ```

3. Reassign disk ownership by using the system ID information obtained from the `disk show` command:

   disk reassign -s *old system ID*

   In the case of the preceding example, the command is: **disk reassign -s 118073209**

   You can respond **Y** when prompted to continue.

4. Verify that the disks were assigned correctly:

   disk show -a

   You must verify that the disks belonging to the replacement node show the new system ID for the replacement node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

   #### Example

   ```
   *> disk show -a
   Local System ID: 118065481

     DISK     OWNER          POOL   SERIAL NUMBER  HOME
   -------    -------------  -----  -------------  -------------
   system-1  (118065481)     Pool0  J8Y0TDZC       system-1  (118065481)
   ```

```
system-1  (118065481)     Pool0  J8Y09DXC       system-1  (118065481)
.
.
.
```

5. If the replacement node is in Maintenance mode (showing the *> prompt), exit Maintenance mode:

   halt

   After you issue the command, you must wait until the system stops at the LOADER prompt.

6. If you are running Data ONTAP 8.2.2 or earlier, on the replacement node at the prompt, confirm that the new controller module boots in clustered Data ONTAP:

   setenv bootarg.init.boot_clustered true

7. Boot the operating system:

   boot_ontap

Installing licenses for the replacement node in clustered Data ONTAP

You must install new licenses for the replacement node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses will continue to be available to the replacement node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the replacement node as soon as possible.

The licenses keys must be in the 28-character format used by ONTAP 8.2 and later.

You have a 90-day grace period to install the license keys; after the grace period, all old licenses are invalidated. Once a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

Steps

1. If you need new license keys in the Data ONTAP 8.2 format, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   Note: The new license keys that you require are auto-generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, contact technical support.

2. Install each license key:

   system license add -license-code *license-key, license-key...*

3. If you want to remove the old licenses, complete the following substeps:

   a. Check for unused licenses:

      license clean-up -unused -simulate

   b. If the list looks correct, remove the unused licenses:

      license clean-up -unused

Restoring Storage Encryption functionality after controller module replacement

After replacing the controller module for a storage system that you previously configured to use Storage Encryption, you must perform additional steps to restore Storage Encryption functionality in an uninterrupted way.. You can skip this task on storage systems that do not have Storage Encryption enabled.

Steps

1. Access the nodeshell:

   `system node run -node node_name`

2. Enter the following command at the storage system prompt:

   `key_manager setup`

3. Complete the steps in the wizard to configure Storage Encryption.

   Verify that a new passphrase is generated and that you select **Yes** to lock all drives.

4. Repeat steps 1 through 3 on the partner node.

   Do not proceed to the next step until you have completed the Storage Encryption setup wizard on each node.

5. On each node, verify that all disks are rekeyed:

   `disk encrypt show`

   None of the disks should list a key ID of 0x0.

6. On each node, load all authentication keys:

   `key_manager restore -all`

7. On each node, verify that all keys are stored on their key management servers:

   `key_manager query`

   None of the key IDs should have an asterisk next to it.

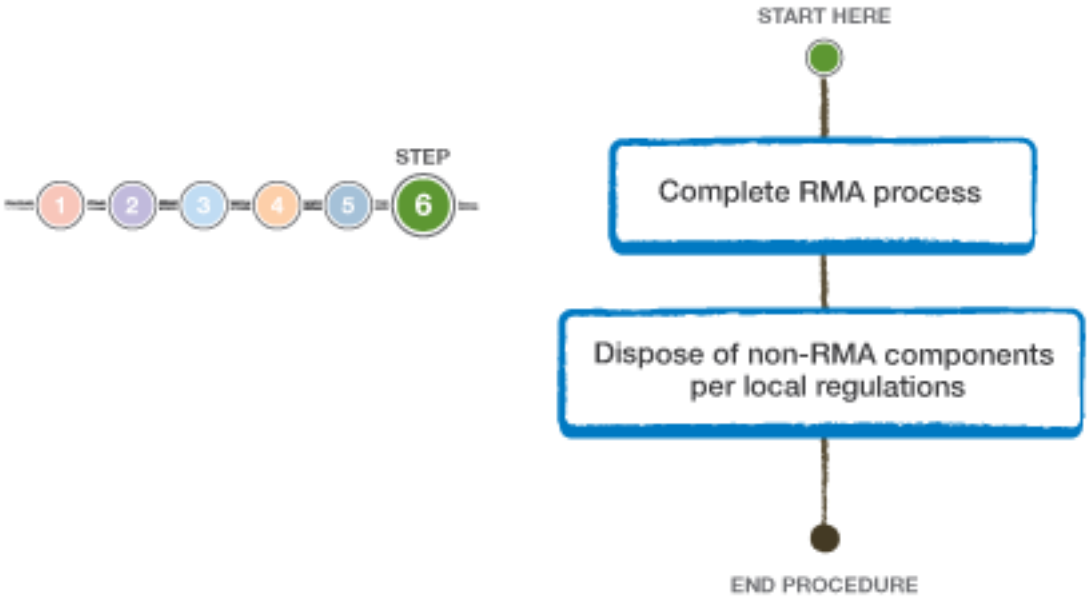
8. Exit the nodeshell and return to the clustershell:

   `exit`

Completing the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at *NetApp Support*, 888-463-8277 (North America), 00-800-44-638277 (Europe), or

+800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.



Disposing of batteries

You must dispose of batteries according to the local regulations regarding battery recycling or disposal. If you cannot properly dispose of batteries, you must return the batteries to NetApp, as described in the RMA instructions that are shipped with the kit.

Related information

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277