NetApp

Upgrading controllers in a MetroCluster FC configuration using switchover and switchback

ONTAP MetroCluster

aherbin, netapp-ivanad, netapp-martyh
April 19, 2021

Table of Contents

Upgrading controllers in a MetroCluster FC configuration using switchover and switchback

You can use the MetroCluster switchover operation to provide nondisruptive service to clients while the controller modules on the partner cluster are upgraded. Other components (such as storage shelves or switches) cannot be upgraded as part of this procedure.

- You can use this procedure only for controller upgrade.

  Other components in the configuration, such as storage shelves or switches, cannot be upgraded at the same time.

- You can use this procedures with certain ONTAP versions:

  ◦ Two-node configurations are supported in ONTAP 9.3 and later.

  ◦ Four and eight node configurations are supported in ONTAP 9.8 and later.

    Do not use this procedure on four- or eight-node configurations running ONTAP versions prior to 9.8.

- Your original and new platforms must be compatible and supported.

  NetApp Hardware Universe

  > **ⓘ** If the original or new platforms are 8020 systems using ports 1c / 1d in FC-VI mode, contact technical support.

- This procedure applies to controller modules in a MetroCluster FC configuration (a two-node stretch MetroCluster or a two or four-node fabric-attached MetroCluster configuration).

- All controllers in the configuration should be upgraded during the same maintenance period.

  Operating the MetroCluster configuration with different controller types is not supported outside of this maintenance activity.

- The supported upgrade path depends on the original platform model.

  Platform models with internal shelves are not supported.

Old platform model	New platform model
• FAS80xx • FAS8200	• FAS8300 • FAS8700
• AFF A300	• AFF A400 • AFF A700

- Mapping of storage, FC and Ethernet connections between original nodes and new nodes in advance is recommended.

- If the new platform has fewer slots than the original system, or if it has fewer or different types of ports, you

might need to add an adapter to the new system.

For more information, see the NetApp Hardware Universe

The following example names are used in this procedure:

- site_A
  - Before upgrade:
    - node_A_1-old
    - node_A_2-old
  - After upgrade:
    - node_A_1-new
    - node_A_2-new
- site_B
  - Before upgrade:
    - node_B_1-old
    - node_B_2-old
  - After upgrade:
    - node_B_1-new
    - node_B_2-new

Preparing for the upgrade

Before making any changes to the existing MetroCluster configuration, you must check the health of the configuration, prepare the new platforms, and perform other miscellaneous tasks.

Verifying the health of the MetroCluster configuration

You must verify the health and connectivity of the MetroCluster configuration prior to performing the upgrade.

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:

   a. Check whether the nodes are multipathed:
      `node run -node node-name sysconfig -a`

      You should issue this command for each node in the MetroCluster configuration.

   b. Verify that there are no broken disks in the configuration:
      `storage disk show -broken`

      You should issue this command on each node in the MetroCluster configuration.

   c. Check for any health alerts:

```
system health alert show
```

You should issue this command on each cluster.

d. Verify the licenses on the clusters:
```
system license show
```

You should issue this command on each cluster.

e. Verify the devices connected to the nodes:

```
network device-discovery show
```

You should issue this command on each cluster.

f. Verify that the timezone and time is set correctly on both sites:
```
cluster date show
```

You should issue this command on each cluster. You can use the `cluster date` commands to configure the time and timezone.

2. Check for any health alerts on the switches (if present):

```
storage switch show
```

You should issue this command on each cluster.

3. Confirm the operational mode of the MetroCluster configuration and perform a MetroCluster check.

a. Confirm the MetroCluster configuration and that the operational mode is normal:
```
metrocluster show
```

b. Confirm that all expected nodes are shown:
```
metrocluster node show
```

c. Issue the following command:
```
metrocluster check run
```

d. Display the results of the MetroCluster check:
```
metrocluster check show
```

4. Check the MetroCluster cabling with the Config Advisor tool.

a. Download and run Config Advisor.

NetApp Downloads: Config Advisor

b. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Mapping ports from the old nodes to the new nodes

You must plan the mapping of the LIFs on physical ports on the old nodes to the physical ports on the new nodes.

When the new node is first booted during the upgrade process, it will replay the most recent configuration of

the old node it is replacing. When you boot node_A_1-new, ONTAP attempts to host LIFs on the same ports that were used on node_A_1-old. Therefore, as part of the upgrade you must adjust the port and LIF configuration so it is compatible with that of the old node. During the upgrade procedure, you will perform steps on both the old and new nodes to ensure correct cluster, management, and data LIF configuration.

The following table shows examples of configuration changes related to the port requirements of the new nodes.

Cluster interconnect physical ports		
Old controller	New controller	Required action
e0a, e0b	e3a, e3b	No matching port. After upgrade, you must recreate cluster ports.
e0c, e0d	e0a,e0b,e0c,e0d	e0c and e0d are matching ports. You do not have to change the configuration, but after upgrade you can spread your cluster LIFs across the available cluster ports.

Steps

1. Determine what physical ports are available on the new controllers and what LIFs can be hosted on the ports.

   The controller's port usage depends on the platform module and which switches you will use in the MetroCluster IP configuration. You can gather the port usage of the new platforms from the NetApp Hardware Universe.

   Also identify the FC-VI card slot usage.

2. Plan your port usage and, if desired, fill in the following tables for reference for each of the new nodes.

   You will refer to the table as you carry out the upgrade procedure.

	node_A_1-old			node_A_1-new		
LIF	Ports	IPspaces	Broadcast domains	Ports	IPspaces	Broadcast domains
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node management						

	node_A_1-old			node_A_1-new		
Cluster management						
Data 1						
Data 2						
Data 3						
Data 4						
SAN						
Intercluster port						

Gathering information before the upgrade

Before upgrading, you must gather information for each of the nodes, and, if necessary, adjust the network broadcast domains, remove any VLANs and interface groups, and gather encryption information.

This task is performed on the existing MetroCluster FC configuration.

Steps

1. Label the cables for the existing controllers, to allow easy identification of cables when setting up the new controllers.

2. Gather the system IDs of the nodes in the MetroCluster configuration:

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   During the replacement procedure you will replace these system IDs with the system IDs of the new controller modules.

   In this example for a four-node MetroCluster FC configuration, the following old system IDs are retrieved:

   - node_A_1-old: 4068741258
   - node_A_2-old: 4068741260
   - node_B_1-old: 4068741254
   - node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                              node
node-systemid        ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
----------          ------------------------ ------------------
-------------                   -------------------
-------------------                   ---------------------
1                       Cluster_A                    Node_A_1-old
4068741258            4068741260                         4068741256
4068741256
1                       Cluster_A                    Node_A_2-old
4068741260            4068741258                         4068741254
4068741254
1                       Cluster_B                    Node_B_1-old
4068741254            4068741256                         4068741258
4068741260
1                       Cluster_B                    Node_B_2-old
4068741256            4068741254                         4068741260
4068741258
4 entries were displayed.
```

In this example for a two-node MetroCluster FC configuration, the following old system IDs are retrieved:

- node_A_1: 4068741258
- node_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster     node      node-systemid dr-partner-systemid
----------- ---------- --------   ------------- -----------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Gather port and LIF information for each node.

   You should gather the output of the following commands for each node:

   - `network interface show -role cluster,node-mgmt`

   - `network port show -node node-name -type physical`

   - `network port vlan show -node node-name`

- ◦ `network port ifgrp show -node node_name -instance`
- ◦ `network port broadcast-domain show`
- ◦ `network port reachability show -detail`
- ◦ `network ipspace show`
- ◦ `volume show`
- ◦ `storage aggregate show`
- ◦ `system node run -node node-name sysconfig -a`

4. If the MetroCluster nodes are in a SAN configuration, collect the relevant information.

   You should gather the output of the following commands:

   - ◦ `fcp adapter show -instance`
   - ◦ `fcp interface show -instance`
   - ◦ `iscsi interface show`
   - ◦ `ucadmin show`

5. If the root volume is encrypted, collect and save the passphrase used for key-manager:

   `security key-manager backup show`

6. If the MetroCluster nodes are using encryption for volumes or aggregates, copy information about the keys and passphrases.

   For additional information, see Backing up onboard key management information manually.

   a. If Onboard Key Manager is configured:
      `security key-manager onboard show-backup`

      You will need the passphrase later in the upgrade procedure.

   b. If enterprise key management (KMIP) is configured, issue the following commands:
      `security key-manager external show -instance`

      `security key-manager key query`

Removing the existing configuration from the Tiebreaker or other monitoring software

If the existing configuration is monitored with the MetroCluster Tiebreaker configuration or other third-party applications (for example, ClusterLion) that can initiate a switchover, you must remove the MetroCluster configuration from the Tiebreaker or other software prior to transition.

Steps

1. Remove the existing MetroCluster configuration from the Tiebreaker software.

   Removing MetroCluster configurations

2. Remove the existing MetroCluster configuration from any third-party application that can initiate switchover.

   Refer to the documentation for the application.

Sending a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

Steps

1. To prevent automatic support case generation, send an Autosupport message to indicate maintenance is underway.

   a. Issue the following command:
      `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      `maintenance-window-in-hours` specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

      `system node autosupport invoke -node * -type all -message MAINT=end`
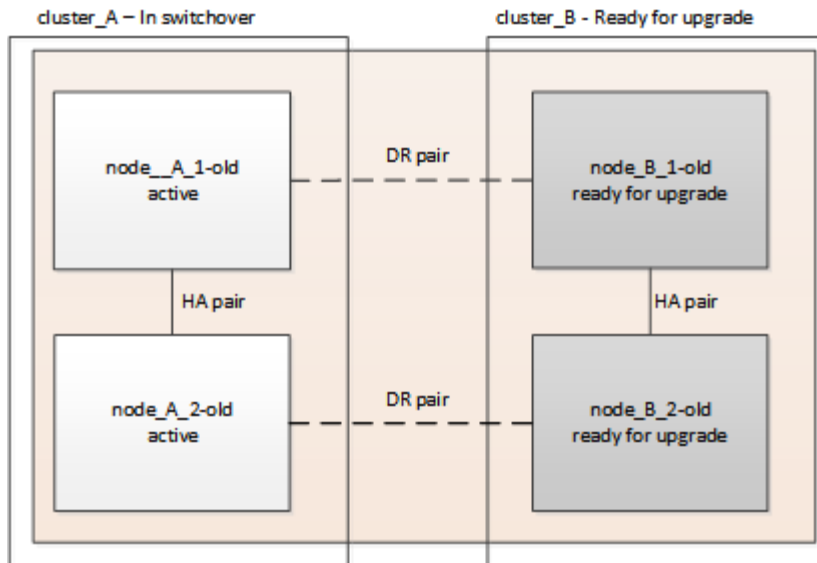
   b. Repeat the command on the partner cluster.

Switching over the MetroCluster configuration

You must switch over the configuration to site_A so that the platforms on site_B can be upgraded.

This task must be performed on site_A.

After completing this task, cluster_A is active and serving data for both sites. cluster_B is inactive, and ready to begin the upgrade process, as shown in the following illustration.

cluster_A – In switchover   cluster_B - Ready for upgrade

node__A_1-old   DR pair   node_B_1-old
active   ready for upgrade

HA pair   HA pair

node_A_2-old   DR pair   node_B_2-old
active   ready for upgrade

Steps

1. Switch over the MetroCluster configuration to site_A so that site_B's nodes can be upgraded:

   a. Issue the following command on cluster_A:
      metrocluster switchover -controller-replacement true

      The operation can take several minutes to complete.

   b. Monitor the switchover operation:
      metrocluster operation show

   c. After the operation is complete, confirm that the nodes are in switchover state:
      metrocluster show

   d. Check the status of the MetroCluster nodes:
      metrocluster node show

2. Heal the data aggregates.

   a. Heal the data aggregates:
      metrocluster heal data-aggregates

   b. Confirm the heal operation is complete by running the `metrocluster operation show` command on the healthy cluster:

      ```
      cluster_A::> metrocluster operation show
        Operation: heal-aggregates
            State: successful
       Start Time: 7/29/2020 20:54:41
         End Time: 7/29/2020 20:54:42
           Errors: -
      ```

3. Heal the root aggregates.

   a. Heal the data aggregates:
      metrocluster heal root-aggregates

b. Confirm the heal operation is complete by running the `metrocluster operation show` command on the healthy cluster:

```
cluster_A::> metrocluster operation show
    Operation: heal-root-aggregates
        State: successful
   Start Time: 7/29/2020 20:58:41
     End Time: 7/29/2020 20:59:42
       Errors: -
```

Preparing the network configuration of the old controllers

To ensure that the networking resumes cleanly on the new controllers, you must move LIFs to a common port and then remove the networking configuration of the old controllers.

- This task must be performed on each of the old nodes.
- You will use the information gathered in Mapping ports from the old nodes to the new nodes.

Steps

1. Boot the old nodes and then log in to the nodes:

   boot_ontap

2. Assign the home port of all data LIFs on the old controller to a common port that is the same on both the old and new controller modules.

   a. Display the LIFs:
      network interface show

      All data LIFS including SAN and NAS will be admin up and operationally down since those are up at switchover site (cluster_A).

   b. Review the output to find a common physical network port that is the same on both the old and new controllers that is not used as a cluster port.

      For example, e0d is a physical port on old controllers and is also present on new controllers. e0d is not used as a cluster port or otherwise on the new controllers.

      For port usage for platform models, see the NetApp Hardware Universe

   c. Modify all data LIFS to use the common port as the home port:

      network interface modify -vserver *svm-name* -lif *data-lif* -home-port *port-id*

      In our example this is e0d.

      For example:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modify broadcast domains to remove vlan and physical ports that need to be deleted:

   broadcast-domain remove-ports -broadcast-domain *broadcast-domain-name* **-ports** *node-name:port-id*

   Repeat this step for all VLAN and physical ports.

4. Remove any VLAN ports using cluster ports as member ports and ifgrps using cluster ports as member ports.

   a. Delete VLAN ports:
      network port vlan delete -node *node-name* **-vlan-name** *portid-vlandid*

      For example:

      ```
      network port vlan delete -node node1 -vlan-name e1c-80
      ```

   b. Remove physical ports from the interface groups:
      network port ifgrp remove-port -node *node-name* **-ifgrp** *interface-group-name* **-port** *portid*

      For example:

      ```
      network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
      ```

   c. Remove VLAN and interface group ports from broadcast domain::
      network port broadcast-domain remove-ports -ipspace *ipspace* **-broadcast -domain** *broadcast-domain-name* **-ports** *nodename:portname,nodename:portname,..*

   d. Modify interface group ports to use other physical ports as member as needed.:
      ifgrp add-port -node *node-name* **-ifgrp** *interface-group-name* **-port** *port-id*

5. Halt the nodes:

   halt -inhibit-takeover true -node *node-name*

   This step must be performed on both nodes.

Removing the old platforms

The old controllers must be removed from the configuration.

This task is performed on site_B.

Steps

1. Connect to the serial console of the old controllers (node_B_1-old and node_B_2-old) at site_B and verify it

is displaying the LOADER prompt.

2. Disconnect the storage and network connections on node_B_1-old and node_B_2-old and label the cables so they can be reconnected to the new nodes.

3. Disconnect the power cables from node_B_1-old and node_B_2-old.

4. Remove the node_B_1-old and node_B_2-old controllers from the rack.

Configuring the new controllers

You must rack and install the controllers, perform required setup in Maintenance mode, and then boot the controllers, and verify the LIF configuration on the controllers.

Setting up the new controllers

You must rack and cable the new controllers.

Steps

1. Plan out the positioning of the new controller modules and storage shelves as needed.

   The rack space depends on the platform model of the controller modules, the switch types, and the number of storage shelves in your configuration.

2. Properly ground yourself.

3. Install the controller modules in the rack or cabinet.

   AFF and FAS Documentation Center

4. If the new controller modules did not come with FC-VI cards of their own and if FC-VI cards from old controllers are compatible on new controllers, swap FC-VI cards and install those in correct slots.

   See the NetApp Hardware Universe for slot info for FC-VI cards.

5. Cable the controllers' power, serial console and management connections as described in the *MetroCluster Installation and Configuration Guides*.

   Do not connect any other cables that were disconnected from old controllers at this time.

   AFF and FAS Documentation Center

6. Power up the new nodes and press Ctrl-C when prompted to display the LOADER prompt.

Netbooting the new controllers

After you install the new nodes, you need to netboot to ensure the new nodes are running the same version of ONTAP as the original nodes. The term netboot means you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you must put a copy of the ONTAP 9 boot image onto a web server that the system can access.

This task is performed on each of the new controller modules.

1. Access the NetApp Support Site to download the files used for performing the netboot of the system.

2. Download the appropriate ONTAP software from the software download section of the NetApp Support Site and store the ontap-version_image.tgz file on a web-accessible directory.

3. Change to the web-accessible directory and verify that the files you need are available.

If the platform model is…	Then…
FAS/AFF8000 series systems	Extract the contents of the ontap-version_image.tgzfile to the target directory: tar -zxvf ontap-version_image.tgz ⓘ If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image.Your directory listing should contain a netboot folder with a kernel file:netboot/kernel Your directory listing should contain a netboot folder with a kernel file: netboot/kernel
All other systems	Your directory listing should contain a netboot folder with a kernel file: ontap-version_image.tgz You do not need to extract the ontap-version_image.tgz file.

4. At the LOADER prompt, configure the netboot connection for a management LIF:

   - If IP addressing is DHCP, configure the automatic connection: `ifconfig e0M -auto`

   - If IP addressing is static, configure the manual connection: `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

5. Perform the netboot.

   - If the platform is an 80xx series system, use this command: `netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

   - If the platform is any other system, use this command: `netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

6. From the boot menu, select option \(7\) **Install new software first** to download and install the new software image to the boot device.

   ```
   Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   ```

7. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL of the image file: `http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

```
Enter username/password if applicable, or press Enter to continue.
```

8. Be sure to enter `n` to skip the backup recovery when you see a prompt similar to the following:

```
Do you want to restore the backup configuration now? {y|n} **n**
```

9. Reboot by entering `y` when you see a prompt similar to the following:

```
    The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n}
// end include reference
```

Clearing the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the configuration.

1. If necessary, halt the node to display the LOADER prompt: `halt`

2. At the LOADER prompt, set the environmental variables to default values: `set-defaults`

3. Save the environment: `saveenv``bye`

4. At the LOADER prompt, launch the boot menu: `boot_ontap menu`

5. At the boot menu prompt, clear the configuration: `wipeconfig`

   Respond `yes` to the confirmation prompt.

   The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

   Respond `yes` to the confirmation prompt.

Restoring the HBA configuration

Depending on the presence and configuration of HBA cards in the controller module, you need to configure them correctly for your site's usage.

Steps

1. In Maintenance mode configure the settings for any HBAs in the system:

   a. Check the current settings of the ports: **ucadmin show**

   b. Update the port settings as needed.

If you have this type of HBA and desired mode…	Use this command…
CNA FC	`ucadmin modify -m fc -t initiator adapter-name`
CNA Ethernet	`ucadmin modify -mode cna adapter-name`
FC target	`fcadmin config -t target adapter-name`
FC initiator	`fcadmin config -t initiator adapter-name`

2. Exit Maintenance mode: **halt**

   After you run the command, wait until the node stops at the LOADER prompt.

3. Boot the node back into Maintenance mode to enable the configuration changes to take effect: **boot_ontap maint**

4. Verify the changes you made:

If you have this type of HBA…	Use this command…
CNA	`ucadmin show`
FC	`fcadmin show`

Setting the HA state on the new controllers and chassis

You must verify the HA state of the controllers and chassis, and, if necessary, update the state to match your system configuration.

Steps

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

   ha-config show

   The HA state for all components should be mcc.

If the MetroCluster configuration has…	The HA state should be…
Two nodes	mcc-2n
Four or eight nodes	mcc

2. If the displayed system state of the controller is not correct, set the HA state for the controller module and chassis:

If the MetroCluster configuration has…	Issue these commands…

Two nodes	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Four or eight nodes	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Reassigning root aggregate disks

Reassign the root aggregate disks to the new controller module, using the sysids gathered earlier

This task is performed in Maintenance mode.

The old system IDs were identified in Gathering information before the upgrade.

The examples in this procedure use controllers with the following system IDs:

Node	Old system ID	New system ID
node_B_1	4068741254	1574774970

Steps

1. Cable all other connections to the new controller modules (FC-VI, storage, cluster interconnect, etc.).
2. Halt the system and boot to Maintenance mode from the LOADER prompt:

   `boot_ontap maint`

3. Display the disks owned by node_B_1-old:

   `disk show -a`

   The command output shows the system ID of the new controller module (1574774970). However, the root aggregate disks are still owned by the old system ID (4068741254). This example does not show drives owned by other nodes in the MetroCluster configuration.

```
*> disk show -a
Local System ID: 1574774970

  DISK          OWNER                        POOL   SERIAL NUMBER    HOME
DR HOME
-----------   -------------             -----  -------------
-------------           -------------
...
rr18:9.126L44 node_B_1-old(4068741254)    Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)    Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)    Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)    Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)    Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)    Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Reassign the root aggregate disks on the drive shelves to the new controller:

   disk reassign -s *old-sysid* -d *new-sysid*

   The following example shows reassignment of drives:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Check that all disks are reassigned as expected:

disk show

```
*> disk show
Local System ID: 1574774970

  DISK          OWNER                          POOL    SERIAL NUMBER    HOME
DR HOME
-----------   -------------                    -----   -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)    Pool1   PZHYN0MD
node_B_1-new(1574774970)   node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)    Pool1   PPG3J5HA
node_B_1-new(1574774970)   node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)    Pool1   PZHTDSZD
node_B_1-new(1574774970)   node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)    Pool0   S0M1J2CF
node_B_1-new(1574774970)   node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)    Pool0   S0M0CQM5
node_B_1-new(1574774970)   node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)    Pool0   S0M1PSDW
node_B_1-new(1574774970)   node_B_1-new(1574774970)
*>
```

6. Display the aggregate status:

aggr status

```
*> aggr status
            Aggr                    State          Status              Options
aggr0_node_b_1-root     online        raid_dp, aggr     root, nosnap=on,
                                mirrored
mirror_resync_priority=high(fixed)
                                fast zeroed
                                64-bit
```

7. Repeat the above steps on the partner node (node_B_2-new).

Booting up the new controllers

You must reboot the controllers from the boot menu to update the controller flash image. Additional steps are required if encryption is configured.

This task must be performed on all the new controllers.

Steps

1. Halt the node:

   halt

2. If external key manager is configured, set the related bootargs:

   setenv bootarg.kmip.init.ipaddr *ip-address*

   setenv bootarg.kmip.init.netmask *netmask*

   setenv bootarg.kmip.init.gateway *gateway-address*

   setenv bootarg.kmip.init.interface *interface-id*

3. Display the boot menu:

   boot_ontap menu

4. If root encryption is used, issue the boot menu command for your key management configuration.

If you are using…	Issue this command at the boot menu prompt…
Onboard key management	recover_onboard_keymanager
External key management	recover_external_keymanager

5. If autoboot is enabled, interrupt autoboot by pressing control-C.

6. From the boot menu, run option (6).

    ℹ   Option 6 will reboot the node twice before completing

Respond y to the system id change prompts. Wait for the second reboot messages:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Double-check that the partner-sysid is the correct:

printenv partner-sysid

If the partner-sysid is not correct, set it:

setenv partner-sysid *partner-sysID*

8. If root encryption is used, again issue the boot menu command for your key management configuration.

If you are using…	Issue this command at the boot menu prompt…
Onboard key management	recover_onboard_keymanager
External key management	recover_external_keymanager

You may need to issue the recover_xxxxxxxx_keymanager command and option 6 at the boot menu prompt multiple times until the nodes fully boot.

9. Boot the nodes:

boot_ontap

10. Wait for the replaced nodes to boot up.

If either node is in takeover mode, perform a giveback using the `storage failover giveback` command.

11. Verify that all ports are in a broadcast domain:

a. View the broadcast domains:
   network port broadcast-domain show

b. Add any ports to a broadcast domain as needed.

   Adding or removing ports from a broadcast domain

c. Add the physical port that will host the intercluster LIFs to the corresponding Broadcast domain.

d. Modify intercluster LIFs to use the new physical port as home port.

e. After the intercluster LIFs are up, check the cluster peer status and re-establish cluster peering as needed.

You may need to reconfigure cluster peering.

[Creating a cluster peer relationship](#)

f. Recreate VLANs and interface groups as needed.

VLAN and interface group membership might be different than that of the old node.

[Creating a VLAN](#)

[Combining physical ports to create interface groups](#)

12. If encryption is used, restore the keys using the correct command for your key management configuration.

If you are using…	Use this command…
Onboard key management	`security key-manager onboard sync` For more information, see [Restoring onboard key management encryption keys](#).
External key management	`security key-manager external restore -vserver SVM -node node -key-server host_name|IP_address:port -key-id key_id -key-tag key_tag node-name` For more information, see [Restoring external key management encryption keys](#).

Verifying LIF configuration

Verify that LIFs are hosted on appropriate node/ports prior to switchback. The following steps need to be performed

This task is performed on site_B, where the nodes have been booted up with root aggregates.

Steps

1. Verify that LIFs are hosted on the appropriate node and ports prior to switchback.

   a. Change to the advanced privilege level:
   `set -privilege advanced`

   b. Override the port configuration to ensure proper LIF placement:
   `vserver config override -command "network interface modify -vserver vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node new_node_name"`

   When entering the network interface modify command within the `vserver config override` command, you cannot use the tab autocomplete feature. You can create the `network interface`

`modify` using autocomplete and then enclose it in the `vserver config override` command.

   c. Return to the admin privilege level:
      set -privilege admin

2. Revert the interfaces to their home node:

   network interface revert * -vserver *vserver-name*

   Perform this step on all SVMs as required.

Switching back the MetroCluster configuration

After the new controllers have been configured, you switch back the MetroCluster configuration to return the configuration to normal operation.

In this task, you will perform the switchback operation, returning the MetroCluster configuration to normal operation. The nodes on site_A are still awaiting upgrade.
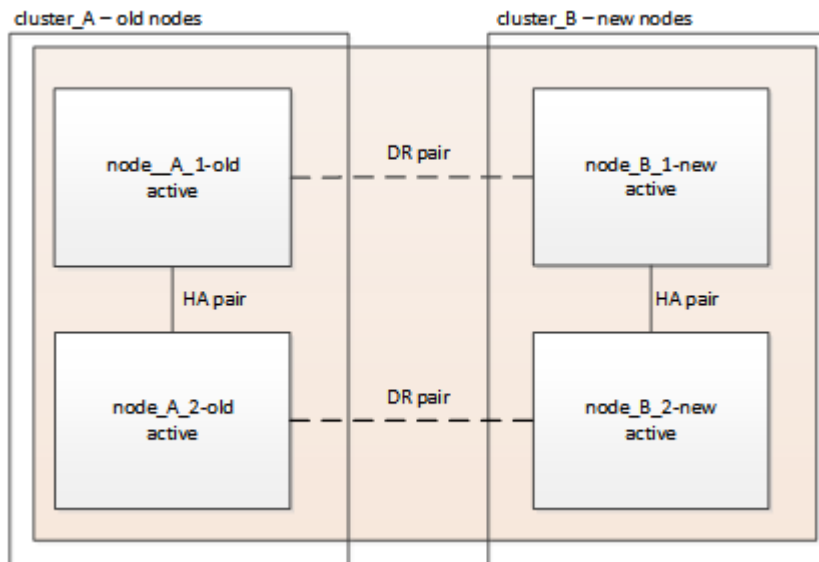
Steps

1. Issue the `metrocluster node show` command on site_B and check the output.

   a. Verify that the new nodes are represented correctly.

   b. Verify that the new nodes are in "Waiting for switchback state."

2. Switchback the cluster: `metrocluster switchback`

3. Check the progress of the switchback operation:

   metrocluster show

   The switchback operation is still in progress when the output displays `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                         Entry Name          State
------------------------------- ------------------- -----------
 Local: cluster_B               Configuration state configured
                                Mode                switchover
                                AUSO Failure Domain -
 Remote: cluster_A              Configuration state configured
                                Mode                waiting-for-switchback
                                AUSO Failure Domain -
```

The switchback operation is complete when the output displays `normal`:

```
cluster_B::> metrocluster show
Cluster                         Entry Name          State
------------------------------- ------------------- -----------
 Local: cluster_B               Configuration state configured
                                Mode                normal
                                AUSO Failure Domain -
 Remote: cluster_A              Configuration state configured
                                Mode                normal
                                AUSO Failure Domain -
```

If a switchback takes a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command. This command is at the advanced privilege level.

Checking the health of the MetroCluster configuration

After upgrading the controller modules you must verify the health of the MetroCluster configuration.

This task can be performed on any node in the MetroCluster configuration.

Steps

1. Verify the operation of the MetroCluster configuration:

   a. Confirm the MetroCluster configuration and that the operational mode is normal:
      metrocluster show

   b. Perform a MetroCluster check:
      metrocluster check run

   c. Display the results of the MetroCluster check:
      metrocluster check show

Upgrading the nodes on cluster_A

You must repeat the upgrade tasks on cluster_A.

Steps

1. Repeat the steps to upgrade the nodes on cluster_A, beginning with Preparing for the upgrade.

   As you perform the tasks, all example references to the clusters and nodes are reversed. For example, when the example is given to switchover from cluster_A, you will switchover from cluster_B.

Sending a custom AutoSupport message after maintenance

After completing the upgrade, you should send an AutoSupport message indicating the end of maintenance, so automatic case creation can resume.

Steps

1. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.

   a. Issue the following command:
   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

   b. Repeat the command on the partner cluster.

Restoring Tiebreaker monitoring

If the MetroCluster configuration was previously configured for monitoring by the Tiebreaker software, you can restore the Tiebreaker connection.

1. Use the steps in Adding MetroCluster configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*.