



# **Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)**

## **ONTAP MetroCluster**

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

This PDF was generated from [https://docs.netapp.com/us-en/ontap-metrocluster/upgrade/task\\_upgrade\\_controllers\\_in\\_a\\_four\\_node\\_ip\\_mcc\\_us\\_switchover\\_and\\_switchback\\_mcc\\_ip.html](https://docs.netapp.com/us-en/ontap-metrocluster/upgrade/task_upgrade_controllers_in_a_four_node_ip_mcc_us_switchover_and_switchback_mcc_ip.html) on May 31, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later) ..... 1

    Workflow for upgrading controllers in an MetroCluster IP configuration ..... 2

    Preparing for the upgrade ..... 3

    Switching over the MetroCluster configuration ..... 14

    Removing interface configurations and uninstalling the old controllers ..... 15

    Updating the switch RCFs to accommodate the new platforms ..... 16

    Configuring the new controllers ..... 17

    Switching back the MetroCluster configuration ..... 28

    Checking the health of the MetroCluster configuration ..... 30

    Upgrading the nodes on cluster\_A ..... 30

    Restoring Tiebreaker or Mediator monitoring ..... 30

    Sending a custom AutoSupport message after maintenance ..... 31

# Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)

Starting with ONTAP 9.8, 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.

- The platforms must be running ONTAP 9.8 or later.
- This procedure applies to controller modules in a MetroCluster IP configuration.
- The supported upgrade path depends on the original platform model.

Platform models with internal shelves are not supported.

Old platform model	New platform model
<ul style="list-style-type: none"><li>• AFF A320</li></ul>	<ul style="list-style-type: none"><li>• AFF A400</li></ul>
<ul style="list-style-type: none"><li>• FAS8200</li></ul>	<ul style="list-style-type: none"><li>• FAS9000</li><li>• FAS8300</li><li>• FAS8700</li></ul>



AFF A320 platform models are not supported for upgrade when using BES-53248 IP switches.

- 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 new platform must be a different model than the original platform.
- The IP switches must be running a supported firmware version.
- 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.

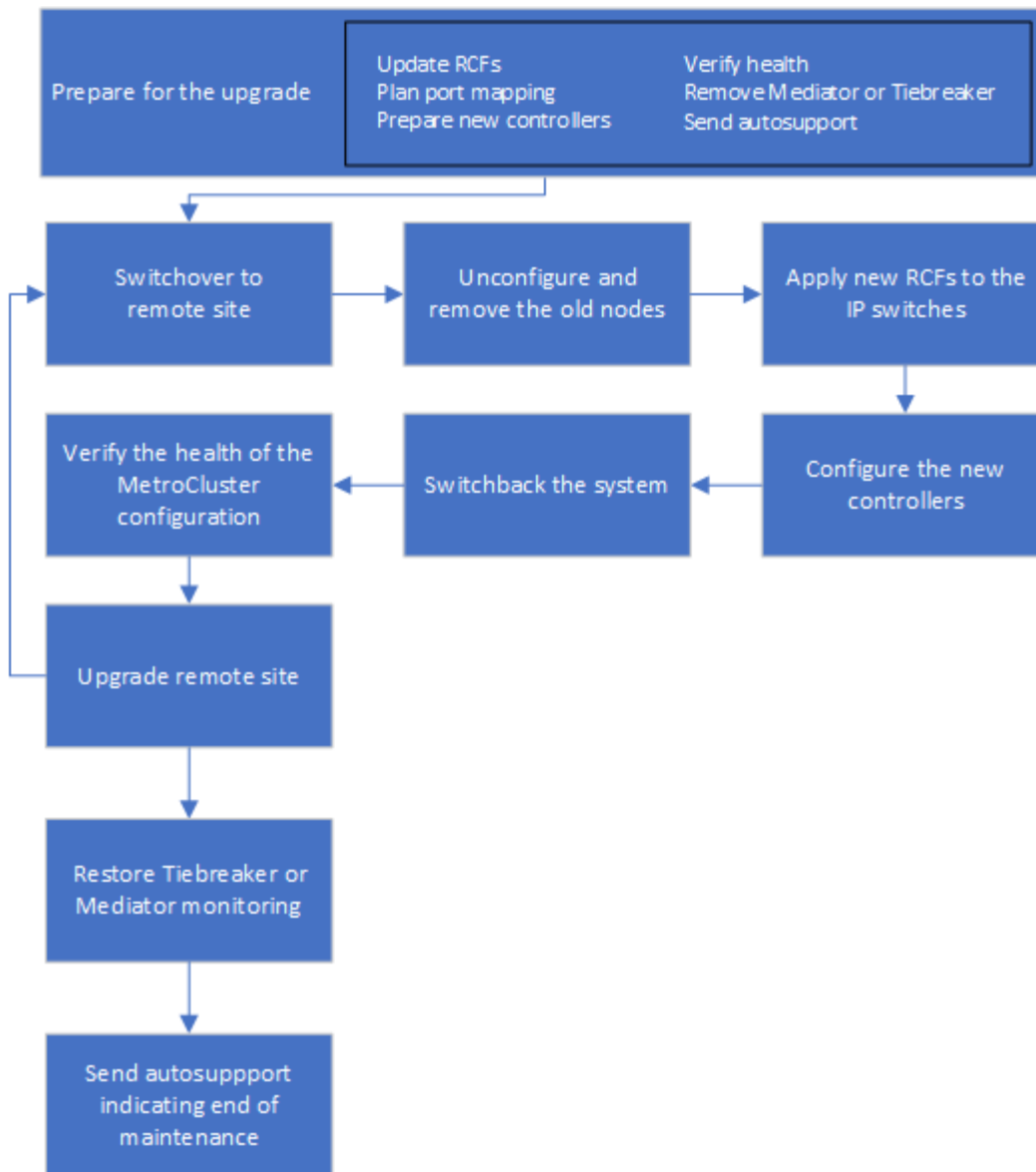
For more information, see the [NetApp Hardware Universe](#).

- You will reuse the IP addresses, netmasks, and gateways of the original platforms on the new platforms.
- 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

## **Workflow for upgrading controllers in an MetroCluster IP configuration**

You can use the workflow diagram to help you plan the upgrade tasks.



## 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.

### Updating the MetroCluster switch RCF files before upgrading controllers

Depending on the old platform models, or if switch configuration is not on the minimum version, or if you want to change VLAN IDs used by the back-end MetroCluster connections, you must update the switch RCF files before you begin the platform upgrade procedure.

You must update the RCF file in the following scenarios:

- For certain platform models, the switches must be using a supported VLAN ID for the back-end MetroCluster IP connections. If the old or new platform models are in the following table, **and not** using a

supported VLAN ID, you must update the switch RCF files.



The local cluster connections can use any VLAN, they do not need to be in the given range.

Platform model (old or new)	Supported VLAN IDs
<ul style="list-style-type: none"><li>AFF A400</li></ul>	<ul style="list-style-type: none"><li>10</li><li>20</li><li>Any value in the range 101 to 4096 inclusive.</li></ul>

- The switch configuration was not configured with minimum supported RCF version:

Switch model	Required RCF file version
Cisco 3132Q-V	1.7 or later
Cisco 3232C	1.7 or later
Broadcom BES-53248	1.3 or later

- You want to change the VLAN configuration.

The VLAN ID range is 101 to 4096 inclusive.

The switches at site\_A will be upgraded when the controllers on site\_A are upgraded.

1. Prepare the IP switches for the application of the new RCF files.

Follow the steps in the section for your switch vendor from the [xref:./upgrade/MetroCluster IP Installation and Configuration Guide](#).

- [Resetting the Broadcom IP switch to factory defaults](#)
- [Resetting the Cisco IP switch to factory defaults](#)

2. Download and install the RCF files.

Follow the steps in the [xref:./upgrade/MetroCluster IP Installation and Configuration Guide](#).

- [Downloading and installing the Broadcom RCF files](#)
- [Downloading and installing the Cisco IP RCF files](#)

## Mapping ports from the old nodes to the new nodes

You must verify that the physical ports on node\_A\_1-old map correctly to the physical ports on node\_A\_1-new, which will allow node\_A\_1-new to communicate with other nodes in the cluster and with the network after the upgrade.

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](#).

2. Plan your port usage and 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						
Cluster management						


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

## 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.

1. Netboot the new controllers:
  - a. Access the [NetApp Support Site](#) to download the files used for performing the netboot of the system.
  - b. 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.
  - c. 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	<p>Extract the contents of the <i>ontap-version_image.tgz</i> file to the target directory:  <code>tar -zxvf ontap-version_image.tgz</code></p> <div>  <p>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</p> </div> <p>Your directory listing should contain a netboot folder with a kernel file:</p> <pre>netboot/kernel</pre>
All other systems	<p>Your directory listing should contain a netboot folder with a kernel file:</p> <p><i>ontap-version_image.tgz</i></p> <p>You do not need to extract the <i>ontap-version_image.tgz</i> file.</p>

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

If IP addressing is...	Then...
DHCP	<p>Configure the automatic connection:</p> <pre>ifconfig e0M -auto</pre>
Static	<p>Configure the manual connection:</p> <pre>ifconfig e0M -addr=ip_addr -mask=netmask</pre> <pre>-gw=gateway</pre>

e. Perform the netboot.

If the platform model is...	Then...
FAS/AFF8000 series systems	<code>netboot</code> <code>http://web_server_ip/path_to_web-accessible_directory/netboot/kernel</code>
All other systems	<code>netboot</code> <code>http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz</code>

- f. 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.

- a. 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.

- a. 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**
```

- a. 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}
```

## 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.

## Verifying MetroCluster health before site upgrade

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. 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
```

3. 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.

## 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.

### Steps

1. Record the physical cabling for each node, labelling cables as needed to allow correct cabling of the new nodes.
2. Gather interconnect, port and LIF information for each node.

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

- `metrocluster interconnect show`
- `metrocluster configuration-settings connection show`
- `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`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

3. Gather the UUIDs for the site\_B (the site whose platforms are currently being upgraded):

```
metrocluster node show -fields node-cluster-uuid, node-uuid
```

These values must be configured accurately on the new site\_B controller modules to ensure a successful upgrade. Copy the values to a file so that you can copy them into the proper commands later in the upgrade process.

The following example shows the command output with the UUIDs:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
(metrocluster node show)
dr-group-id cluster      node      node-uuid
node-cluster-uuid
-----
1              cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1              cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1              cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1              cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::~*
```

It is recommended that you record the UUIDs into a table similar to the following.

Cluster or node	UUID
cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

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

You should gather the output of the following commands:

- `fcv adapter show -instance`

- `fcg 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`**

7. Gather the system IDs of the existing nodes:

**`metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`**

The following output shows the reassigned drives.

```
::> 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	537403324	537403323		
537403321		537403322				
1	cluster_A	node_A_2	537403323	537403324		
537403322		537403321				
1	cluster_B	node_B_1	537403322	537403321		
537403323		537403324				
1	cluster_B	node_B_2	537403321	537403322		
537403324		537403323				

4 entries were displayed.

## Removing Mediator or Tiebreaker monitoring

Before the upgrading the platforms, you must remove monitoring if the MetroCluster configuration is monitored with the Tiebreaker or Mediator utility.

### Steps

1. Collect the output for the following command:

```
storage iscsi-initiator show
```

2. Remove the existing MetroCluster configuration from Tiebreaker, Mediator, or other software that can initiate switchover.

If you are using...	Use this procedure...
<b>Tiebreaker</b>	<a href="#">Removing MetroCluster Configurations</a> in the <i>MetroCluster Tiebreaker Installation and Configuration Guide</i>
<b>Mediator</b>	Issue the following command from the ONTAP prompt:  <pre>metrocluster configuration-settings mediator remove</pre>
<b>Third-party applications</b>	Refer to the product documentation.

## 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. Log in to the cluster.
2. Invoke an AutoSupport message indicating the start of the maintenance:

```
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
```

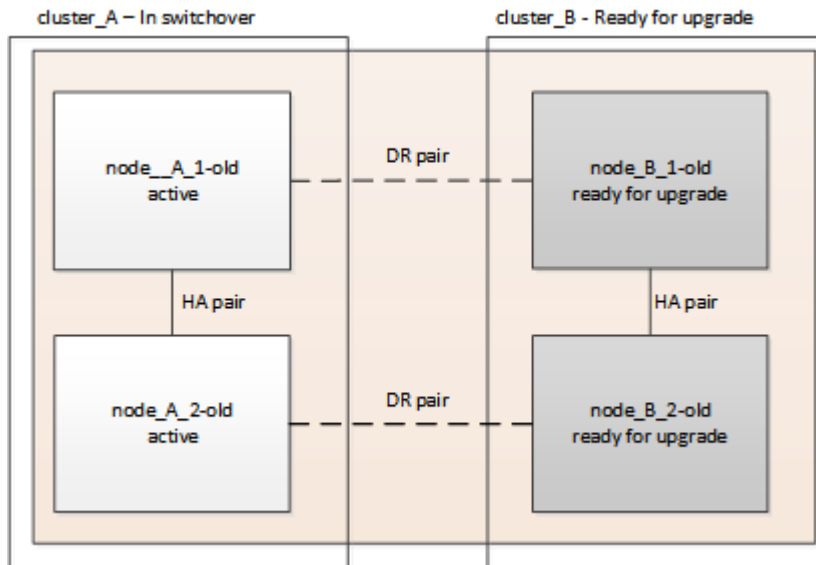
3. Repeat these steps on the partner site.

## 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.



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
```

Automatic healing of aggregates after negotiated switchover is disabled during controller upgrade.



# Removing interface configurations and uninstalling the old controllers

You must move data LIFs to a common port, remove VLANs and interface groups on the old controllers and then physically uninstall the controllers.

- These steps are performed on the old controllers (node\_B\_1-old, node\_B\_2-old).
- See the information you gathered in [Mapping ports from the old nodes to the new nodes](#).

## Steps

1. Boot the old nodes and 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. 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 ala -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
```

4. Halt the nodes to the LOADER prompt:

```
halt -inhibit-takeover true
```

5. 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.

6. Gather the bootarg values:

```
printenv
```

7. 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.

8. Disconnect the power cables from node\_B\_1-old and node\_B\_2-old.

9. Remove the node\_B\_1-old and node\_B\_2-old controllers from the rack.

## Updating the switch RCFs to accommodate the new platforms

You must update the switches to a configuration that supports the new platform models.

You perform this task at the site containing the controllers that are currently being upgraded. In the examples shown in this procedure we are upgrading site\_B first.

The switches at site\_A will be upgraded when the controllers on site\_A are upgraded.

### Steps

1. Prepare the IP switches for the application of the new RCF files.

Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration Guide*.

#### MetroCluster IP installation and configuration

- [Resetting the Broadcom IP switch to factory defaults](#)
- [Resetting the Cisco IP switch to factory defaults](#)

2. Download and install the RCF files.

Follow the steps in the section for your switch vendor from the [MetroCluster IP installation and configuration](#).

- [Downloading and installing the Broadcom RCF files](#)
- [Downloading and installing the Cisco IP RCF files](#)

## 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. Cable the controllers to the IP switches as described in the *MetroCluster IP Installation and Configuration Guide*.

[MetroCluster IP installation and configuration](#)

- [Cabling the IP switches](#)

5. Power up the new nodes and boot them to Maintenance mode.

### 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	<code>ucadmin modify -m fc -t initiator adapter-name</code>
CNA Ethernet	<code>ucadmin modify -mode cna adapter-name</code>
FC target	<code>fcadmin config -t target adapter-name</code>
FC initiator	<code>fcadmin config -t initiator adapter-name</code>

- Exit Maintenance mode: `halt`

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

- Boot the node back into Maintenance mode to enable the configuration changes to take effect:  
`boot_ontap maint`
- Verify the changes you made:

If you have this type of HBA...	Use this command...
CNA	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

## 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

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

```
ha-config show
```

The HA state for all components should be mccip.

- If the displayed system state of the controller or chassis is not correct, set the HA state:

```
ha-config modify controller mccip
```

```
ha-config modify chassis mccip
```

## Setting the MetroCluster IP bootarg variables

Certain MetroCluster IP bootarg values must be configured on the new controller

modules. The values must match those configured on the old controller modules.

In this task, you will use the UUIDs and system IDs identified earlier in the upgrade procedure in [Gathering information before the upgrade](#).

### Steps

1. If the nodes being upgraded are AFF A400, FAS8300, or FAS8700 models, set the following bootargs at the LOADER prompt:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
```

```
setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
```



If the interfaces are using the default VLANs, the vlan-id is not necessary.

The following commands set the values for node\_B\_1-new using VLAN 120 for the first network and VLAN 130 for the second network:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

The following commands set the values for node\_B\_2-new using VLAN 120 for the first network and VLAN 130 for the second network:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

The following example shows the commands for node\_B\_1-new when the default VLAN is used:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

The following example shows the commands for node\_B\_2-new when the default VLAN is used:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. If the nodes being upgraded are not systems listed in the previous step, at the LOADER prompt for each of the surviving nodes, set the following bootargs with local\_IP/mask:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address
```

```
setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address
```

The following commands set the values for node\_B\_1-new:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

The following commands set the values for node\_B\_2-new:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

3. At the new nodes' LOADER prompt, set the UUIDs:

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID
```

```
setenv bootarg.mgwd.cluster_uuid local-cluster-UUID
```

```
setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID
```

```
setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID
```

```
setenv bootarg.mcc.iscsi.node_uuid local-node-UUID .. Set the UUIDs on node_B_1-new.
```

+ The following example shows the commands for setting the UUIDs on node\_B\_1-new:

+

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-00a098908039
```

a. Set the UUIDs on node\_B\_2-new:

The following example shows the commands for setting the UUIDs on node\_B\_2-new:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-
00a098908c35
```

4. If the original systems were configured for ADP, at each of the replacement nodes' LOADER prompt, enable ADP:

```
setenv bootarg.mcc.adp_enabled true
```

5. Set the following variables:

```
setenv bootarg.mcc.local_config_id original-sys-id
```

```
setenv bootarg.mcc.dr_partner dr-partner-sys-id
```



The `setenv bootarg.mcc.local_config_id` variable must be set to the sys-id of the **original** controller module, node\_B\_1-old.

- a. Set the variables on node\_B\_1-new.

The following example shows the commands for setting the values on node\_B\_1-new:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

- b. Set the variables on node\_B\_2-new.

The following example shows the commands for setting the values on node\_B\_2-new:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. If using encryption with external key manager, set the required bootargs:

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

## Reassigning root aggregate disks

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

These steps are performed in Maintenance mode.

### Steps

1. Boot the system to Maintenance mode:

```
boot_ontap maint
```

2. Display the disks on node\_B\_1-new from the Maintenance mode prompt:

```
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 (537403322). 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
-----
prod3-rk18:9.126L44  node_B_1-old(537403322)  Pool1  PZHYN0MD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:9.126L49  node_B_1-old(537403322)  Pool1  PPG3J5HA
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:8.126L21  node_B_1-old(537403322)  Pool1  PZHTDSZD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L2   node_B_1-old(537403322)  Pool10 S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3   node_B_1-old(537403322)  Pool10 S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27  node_B_1-old(537403322)  Pool10 S0M1PSDW
node_B_1-old(537403322)  node_B_1-old(537403322)
.
.
.

```

3. Reassign the root aggregate disks on the drive shelves to the new controllers.

Using ADP?	Command to use
<b>Yes</b>	<code>disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid</code>
<b>No</b>	<code>disk reassign -s old-sysid -d new-sysid</code>

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

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

The following example shows reassignment of drives in a non-ADP configuration:

```
*> disk reassign -s 537403322 -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)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Verify that the disks of the root aggregate are properly reassigned old-remove:

**disk show**

**storage aggr status**

```
*> disk show
Local System ID: 537097247
```

DISK HOME	OWNER DR HOME	POOL	SERIAL NUMBER
----- -----	----- -----	-----	-----
prod03-rk18:8.126L18	node_B_1-new(537097247)	Pool11	PZHYN0MD
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod04-rk18:9.126L49	node_B_1-new(537097247)	Pool11	PPG3J5HA
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod04-rk18:8.126L21	node_B_1-new(537097247)	Pool11	PZHTDSZD
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod02-rk18:8.126L2	node_B_1-new(537097247)	Pool10	S0M1J2CF
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod02-rk18:9.126L29	node_B_1-new(537097247)	Pool10	S0M0CQM5
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod01-rk18:8.126L1	node_B_1-new(537097247)	Pool10	S0M1PSDW
node_B_1-new(537097247)	node_B_1-new(537097247)		

```
::>
```

```
::> aggr status
```

Aggr	State	Status	Options
aggr0_node_B_1	online	raid_dp, aggr	root,
nosnap=on,		mirrored	
mirror_resync_priority=high(fixed)		fast zeroed	
		64-bit	

## Booting up the new controllers

You must boot the new controllers, taking care to ensure that the bootarg variables are correct and, if needed, perform the encryption recovery steps.

### Steps

1. Halt the new nodes:

```
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. Check if the partner-sysid is the current:

```
printenv partner-sysid
```

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

```
setenv partner-sysid partner-sysID
```

4. Display the ONTAP boot menu:

```
boot_ontap menu
```

5. 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	<code>recover_onboard_keymanager</code>
External key management	<code>recover_external_keymanager</code>

6. From the boot menu, select **(6) Update flash from backup config.**



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. On LOADER, double-check the bootarg values and update the values as needed.

Use the steps in [Setting the MetroCluster IP bootarg variables](#).

8. 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
```

9. 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	<code>recover_onboard_keymanager</code>

If you are using...	Issue this command at the boot menu prompt...
External key management	<code>recover_external_keymanager</code>

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

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. 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	<code>security key-manager onboard sync</code>  For more information, see <a href="#">Restoring onboard key management encryption keys</a> .
External key management	<code>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</code>  For more information, see <a href="#">Restoring external key management encryption keys</a> .  +

12. 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. 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](#)

## Verifying and restoring LIF configuration

Verify that LIFs are hosted on appropriate nodes and ports as mapped out at the

beginning of the upgrade procedure.

- This task is performed on site\_B.
- See the port mapping plan you created in [Mapping ports from the old nodes to the new nodes](#).

### 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
```

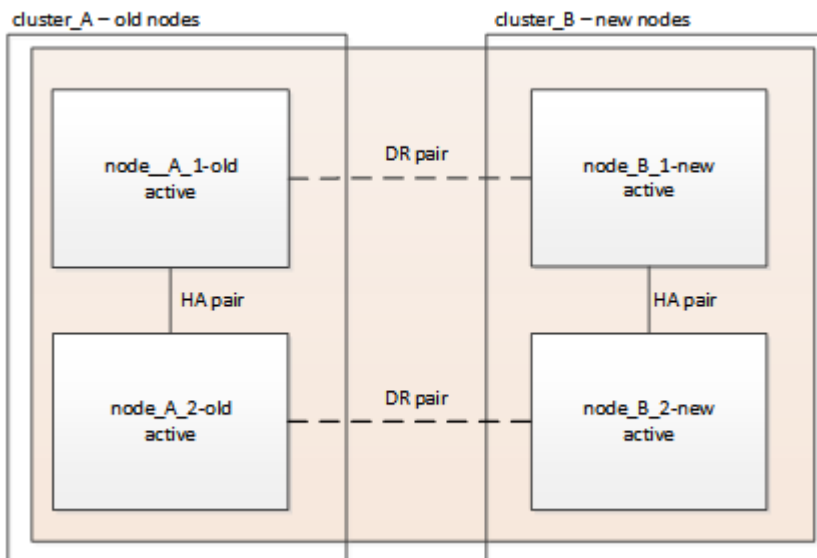
2. Revert the interfaces to their home node:

```
network interface revert * -vserver vserver-name
```

Perform this step on all SVMs as required.

## Switching back the MetroCluster configuration

In this task, you will perform the switchback operation, and the MetroCluster configuration returns 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. Perform the healing and switchback by running the required commands from any node in the active cluster (the cluster that is not undergoing upgrade).
  - a. Heal the data aggregates:  
`metrocluster heal aggregates`
  - b. Heal the root aggregates:  
`metrocluster heal root`
  - c. 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`

2. Verify the MetroCluster connectivity and status.

- a. Check the MetroCluster IP connections:

`storage iscsi-initiator show`

- b. Check that the nodes are operating:

`metrocluster node show`

- c. Check that the MetroCluster IP interfaces are up:

`metrocluster configuration-settings interface show`

- d. Check that local failover is enabled: `storage failover 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.

## Restoring Tiebreaker or Mediator monitoring

After completing the upgrade of the MetroCluster configuration, you can resume



monitoring with the Tiebreaker or Mediator utility.

### Steps

1. Restore monitoring if necessary, using the procedure for your configuration.

If you are using...	Use this procedure
<b>Tiebreaker</b>	<a href="#">Adding MetroCluster configurations</a> in the <i>MetroCluster Tiebreaker Installation and Configuration Guide</i>
<b>Mediator</b>	<a href="#">Configuring the ONTAP Mediator service from a MetroCluster IP configuration</a> in the <i>MetroCluster IP Installation and Configuration Guide</i>
<b>Third-party applications</b>	Refer to the product documentation.

## 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.

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.