



Upgrade or expand the MetroCluster configuration

ONTAP MetroCluster

NetApp
April 13, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap-metrocluster/upgrade/concept_choosing_an_upgrade_method_mcc.html on April 13, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Upgrade or expand the MetroCluster configuration	1
Choosing an upgrade or refresh method	1
Upgrading controllers in a MetroCluster FC configuration using switchover and switchback	3
Upgrade controllers from AFF A700 to AFF A900 in a MetroCluster FC configuration using switchover and switchback (ONTAP 9.10.1 and later)	27
Upgrading controllers in a four-node MetroCluster FC configuration using switchover and switchback with "system controller replace" commands (ONTAP 9.10.1 and later)	53
Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)	70
Upgrade controllers from AFF A700 to AFF A900 in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.10.1 and later)	101
Refreshing a four-node MetroCluster FC configuration	130
Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)	132
Expand a two-node MetroCluster FC configuration to a four-node configuration	136
Expand a four-node MetroCluster FC configuration to an eight-node configuration	173
Expanding a four-node MetroCluster IP configuration to an eight-node configuration	207
Removing a Disaster Recovery group	232
Where to find additional information	237

Upgrade or expand the MetroCluster configuration

Choosing an upgrade or refresh method

The upgrade or refresh procedure you use depends on the platform model, scope of the upgrade, and type of MetroCluster configuration.

There are different types of upgrade and refresh procedures.

- Upgrade procedures apply only to the controller modules. The controllers are replaced with a new controller model.

The storage shelf models are not upgraded.

- In switchover and switchback procedures, the MetroCluster switchover operation is used to provide nondisruptive service to clients while the controller modules on the partner cluster are upgraded.
- In an ARL-based controller upgrade procedure, the aggregate relocation operations are used to nondisruptively move data from the old configuration to the new, upgraded configuration.
- Refresh procedures apply to the controllers and the storage shelves.

In the refresh procedures, new controllers and shelves are added to the MetroCluster configuration, creating a second DR group, and then data is nondisruptively migrated to the new nodes.

The original controllers are then retired.

Choosing a procedure that does not use aggregate relocation

Type of upgrade or refresh	MetroCluster type	First ONTAP version support	Procedure
<ul style="list-style-type: none">• Scope: Platform (controller modules) only• Method: Automated switchover/switchback	FC	9.10.1	Upgrading controllers in a four-node MetroCluster FC configuration using switchover and switchback with "system controller replace" commands (ONTAP 9.10.1 and later)
<ul style="list-style-type: none">• Scope: Platform (controller modules) only• Method: Automated switchover/switchback	IP	9.10.1	Upgrade controllers from AFF A700 to AFF A900 in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.10.1 and later)

<ul style="list-style-type: none"> • Scope: Platform (controller modules) only • Method: Switchover/switchback 	FC	9.8	Upgrading controllers in a MetroCluster FC configuration using switchover and switchback
<ul style="list-style-type: none"> • Scope: Platform (controller modules) only • Method: Switchover/switchback 	IP	9.8	Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)
<ul style="list-style-type: none"> • Scope: Platform (controller modules) and storage shelves • Method: Expand the MetroCluster configuration and then remove the old nodes 	FC	9.6 and later	Refreshing a four-node MetroCluster FC configuration
<ul style="list-style-type: none"> • Scope: Platform (controller modules) and storage shelves • Method: Expand the MetroCluster configuration and then remove the old nodes 	IP	9.8	Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Choosing a procedure using aggregate relocation

Aggregate relocation procedure	MetroCluster type	First ONTAP version support	Procedure
Using system controller replace commands and swapping the controller module and NVM	FC	9.10.1 and later	Use "system controller replace" commands to upgrade AFF A700 to AFF A900 running ONTAP 9.10.1 RC2 or later
Using system controller replace commands	FC	9.8 and later	Using "system controller replace" commands to upgrade controller hardware running ONTAP 9.8 and later

Aggregate relocation procedure	MetroCluster type	First ONTAP version support	Procedure
Using system controller replace commands	FC	9.5 through 9.7	Using “system controller replace” commands to upgrade controller hardware running ONTAP 9.5 to ONTAP 9.7
Using manual ARL commands	FC	9.8	Manually upgrade controller hardware running ONTAP 9.8 and later
Using manual ARL commands	FC	9.7 and earlier	Manually upgrade controller hardware running ONTAP 9.7 and earlier

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.

About this task

- 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 FAS8020 or AFF8020 systems using ports 1c and 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
<ul style="list-style-type: none"> • FAS80x0 • FAS8200 	<ul style="list-style-type: none"> • FAS8300
<ul style="list-style-type: none"> • AFF A300 • AFF80x0 	<ul style="list-style-type: none"> • AFF A400 • AFF A700



Upgrading a FAS8020 or AFF8020 is not supported when using 1c and 1d ports in FC-VI mode.

- 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 time zone and time are 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 time zone.

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.

About this task

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						
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.

About this task

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.

About this task

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.

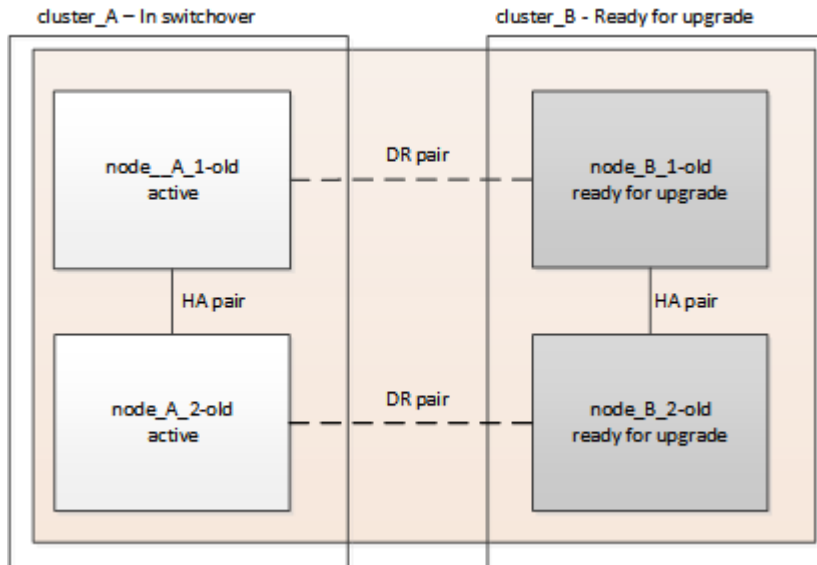
Switching over the MetroCluster configuration

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

About this task

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.



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.

About this task

- 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 the following 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 elc-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
```

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.

About this task

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.

Steps

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. Go 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 <code>ontap-version_image.tgz</code> file to the target directory: <code>tar -zxvf ontap-version_image.tgz</code></p> <p>NOTE: If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image.</p> <p>Your directory listing should contain a netboot folder with a kernel file: <code>netboot/kernel</code></p>
All other systems	<p>Your directory listing should contain a netboot folder with a kernel file: <code>ontap-version_image.tgz</code></p> <p>You do not need to extract the <code>ontap-version_image.tgz</code> file.</p>

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 the following 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}

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}

Clearing the configuration on a controller module

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

Steps

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
```

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

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	<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

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	<code>mcc-2n</code>
Four or eight nodes	<code>mcc</code>

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	<pre>ha-config modify controller mcc-2n ha-config modify chassis mcc-2n</pre>
Four or eight nodes	<pre>ha-config modify controller mcc ha-config modify chassis mcc</pre>

Reassigning root aggregate disks

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

About this task

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)   Pool11 PZHYN0MD
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool11 PPG3J5HA
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool11 PZHTDSZD
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool10 SOM1J2CF
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool10 SOM0CQM5
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool10 SOM1PSDW
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  SOM1J2CF
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  SOM0CQM5
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  SOM1PSDW
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.

About this task

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, depending on the ONTAP version you are using, select the boot menu option or issue the boot menu command for your key management configuration.

- Beginning with ONTAP 9.8, select the boot menu option.

If you are using...	Select this boot menu option...
---------------------	---------------------------------

Onboard key management	Option “10” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.
External key management	Option “11” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.

- In ONTAP 9.7 and earlier, issue the boot menu command.

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>

5. If autoboot is enabled, interrupt autoboot by pressing CTRL-C.
6. From the boot menu, run option “6”.



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 correct:

```
printenv partner-sysid
```

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

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

8. If root encryption is used, depending on the ONTAP version you are using, select the boot menu option or issue the boot menu command again for your key management configuration.
 - Beginning with ONTAP 9.8, select the boot menu option.

If you are using...	Select this boot menu option...
---------------------	---------------------------------

Onboard key management	Option “10” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.
External key management	Option “11” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.

Depending on the key manager setting, perform the recovery procedure by selecting option “10” or option “11”, followed by option “6” at the first boot menu prompt. To boot the nodes completely, you might need to repeat the recovery procedure continued by option “1” (normal boot).

- In ONTAP 9.7 and earlier, issue the boot menu command.

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>

You might need to issue the `recover_XXXXXXX_keymanager` command at the boot menu prompt multiple times until the nodes completely 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:

```
storage failover giveback
```

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

- View the broadcast domains:

```
network port broadcast-domain show
```

- Add any ports to a broadcast domain as needed.

[Adding or removing ports from a broadcast domain](#)

- Add the physical port that will host the intercluster LIFs to the corresponding Broadcast domain.
- Modify intercluster LIFs to use the new physical port as home port.
- After the intercluster LIFs are up, check the cluster peer status and re-establish cluster peering as

needed.

You might 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	<pre>security key-manager onboard sync</pre> <p>For more information, see Restoring onboard key management encryption keys.</p>
External key management	<pre>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</pre> <p>For more information, see Restoring external key management encryption keys.</p>

Verifying LIF configuration

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

About this task

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
```

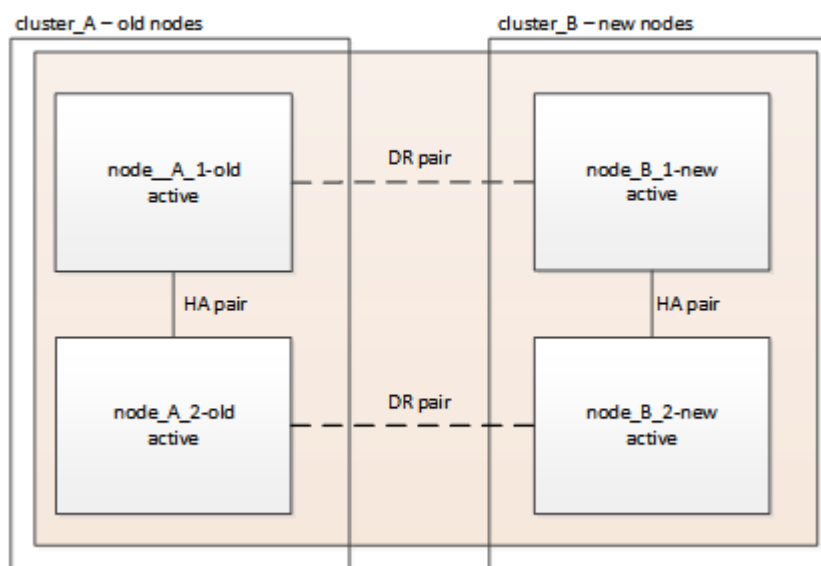
Perform this step on all SVMs as required.

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.

About this task

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.

About this task

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.

Step

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.

Step

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 *MetroCluster Tiebreaker Installation and Configuration*.

Upgrade controllers from AFF A700 to AFF A900 in a MetroCluster FC configuration using switchover and switchback (ONTAP 9.10.1 and later)

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

About this task

- You can use this procedure only for controller upgrade.

You cannot upgrade other components in the configuration, such as storage shelves or switches, at the same time.

- You can use this procedure with ONTAP 9.10.1 and later.
 - Four and eight-node configurations are supported in ONTAP 9.10.1 and later.



The AFF A900 system is only supported in ONTAP 9.10.1 or later.

[NetApp Hardware Universe](#)

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

The following table shows the supported model matrix for the controller upgrade.

Old platform model	New platform model
<ul style="list-style-type: none"> • AFF A700 	<ul style="list-style-type: none"> • AFF A900

- During the upgrade procedure, you are required to change the MetroCluster fabric, including the RCF and physical changes of cabling. You can perform the RCF and cabling changes before performing the controller upgrade.
- This upgrade procedure does not require you do not change the storage, FC, and Ethernet connections between the original nodes and the new nodes.
- During the upgrade procedure, you should not add or remove other cards from the AFF A700 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-A700
 - node_A_2-A700
 - After upgrade:
 - node_A_1-A900
 - node_A_2-A900
- site_B
 - Before upgrade:
 - node_B_1-A700
 - node_B_2-A700
 - After upgrade:
 - node_B_1-A900
 - node_B_2-A900

Prepare for the upgrade

Before making any changes to the existing MetroCluster configuration, you must check the health of the configuration, change the RCF files and cabling to match to new port connectivity topology required for the AFF A900 fabric MetroCluster configuration, and perform other miscellaneous tasks.

Clear slot 7 on the AFF A700 controller

The MetroCluster configuration on an AFF A900 requires 8 FC-VI ports across FC-VI cards in slots 5 and 7. Before starting the upgrade, if there are cards in slot 7 on the AFF A700, you must move them to other slots for all the nodes of the cluster.

Verify the health of the MetroCluster configuration

Before you update the RCF files and cabling for the AFF A900 fabric MetroCluster configuration, you must verify the health and connectivity of the configuration.

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 time zone and time are 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 time zone.

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.

Update the fabric switch RCF files

The AFF A900 fabric MetroCluster requires two four-port FC-VI adapters per node compared to a single four-port FC-VI adapter required by an AFF A700. Before you start the controller upgrade to the AFF A900 controller, you must modify the fabric switch RCF files to support the AFF A900 connection topology.

1. From the [MetroCluster RCF file download page](#), download the correct RCF file for a AFF A900 fabric MetroCluster and the switch model that is in use on the AFF A700 configuration.
2. Update the RCF file on the fabric A switches, switch A1, and switch B1 by following the steps in [Configuring the FC switches](#).



The RCF file update to support the AFF A900 fabric MetroCluster configuration does not affect the port and connections used for the AFF A700 fabric MetroCluster configuration.

3. After updating the RCF files on the fabric A switches, all storage and FC-VI connections should come online. Check the FC-VI connections:

```
metrocluster interconnect mirror show
```

- a. Verify that the local and remote site disks are listed in the `sysconfig` output.

4. You must verify that MetroCluster is in a healthy state after the RCF file update for fabric A switches.

- a. Check metro cluster connections: `metrocluster interconnect mirror show`

- b. Run metrocluster check: `metrocluster check run`

- c. See the MetroCluster run results when the run completes: `metrocluster check show`

5. Update the fabric B switches (switches 2 and 4) by repeating [Step 2](#) to [Step 5](#).

Verify the health of the MetroCluster configuration after the RCF file update

You must verify the health and connectivity of the MetroCluster configuration before 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 time zone and time are 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 time zone.

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.

Map ports from the AFF A700 nodes to the AFF A900 nodes

During the controller upgrade process, you must only change the connections that are mentioned in this procedure.

If the AFF A700 controllers have a card in slot 7, you should move it to another slot before starting the controller upgrade procedure. You must have slot 7 available for the addition of the second FC-VI adapter that is required for the functioning of fabric MetroCluster on the AFF A900.

Gather 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.

About this task

This task is performed on the existing MetroCluster FC configuration.

Steps

1. Gather the MetroCluster configuration node system IDs:

```
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 controller modules.

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

- node_A_1-A700: 537037649
- node_A_2-A700: 537407030
- node_B_1-A700: 0537407114

◦ node_B_2-A700: 537035354

```
Cluster_A::*> 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  nodeA_1-A700    537407114      537035354
537411005          537410611
1          Cluster_A  nodeA_2-A700    537035354      537407114
537410611          537411005
1          Cluster_B  nodeB_1-A700    537410611      537411005
537035354          537407114
1          Cluster_B  nodeB_2-A700    537411005

4 entries were displayed.
```

2. 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

3. 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

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

```
security key-manager backup show
```

5. 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
```

Remove 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.

[Remove MetroCluster configurations](#)

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

Refer to the documentation for the application.

Send 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.

About this task

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.

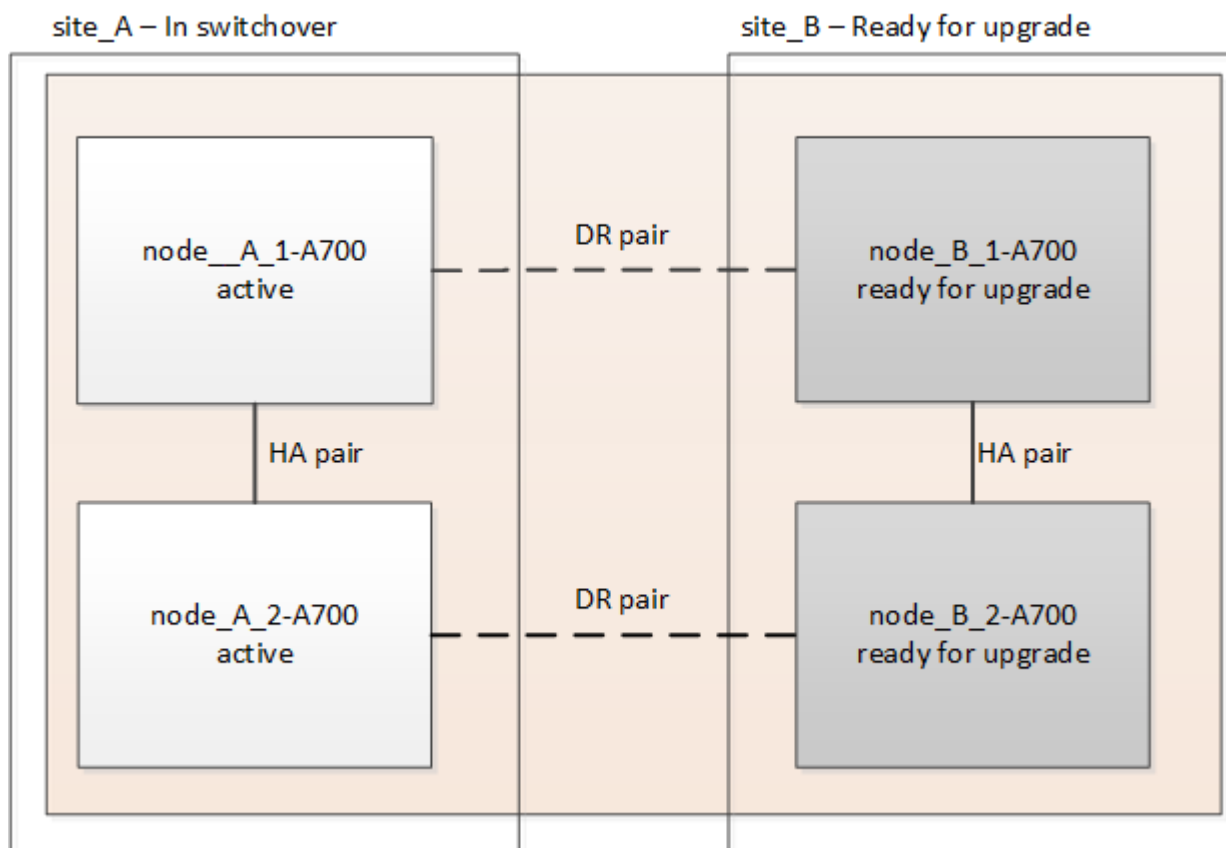
Switch over the MetroCluster configuration

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

About this task

This task must be performed on site_A.

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



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 site_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: -
```

Remove the AFF A700 controller module and NVS at site_B

You must remove the old controllers from the configuration.

You perform this task on site_B.

Before you begin

If you are not already grounded, properly ground yourself.

Steps

- 1. Connect to the serial console of the old controllers (node_B_1-700 and node_B_2-700) at site_B and verify it is displaying the `LOADER` prompt.
- 2. Gather the bootarg values from both nodes at site_B: `printenv`
- 3. Power off the chassis at site_B.

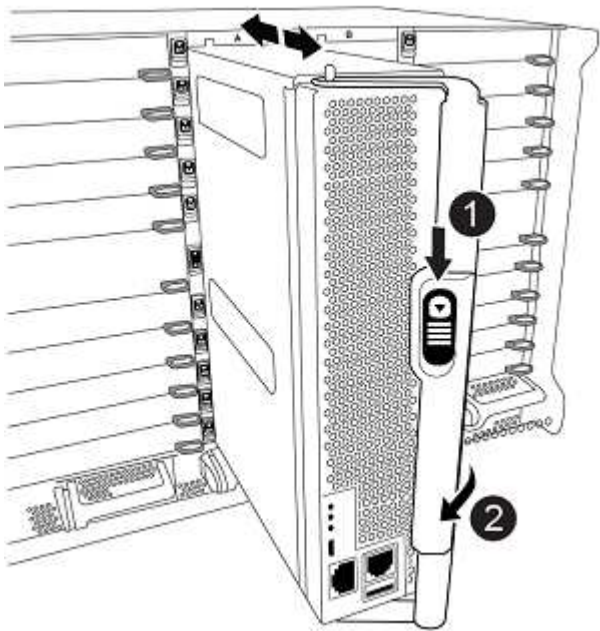
Remove the controller module and NVS from both nodes at site_B

Remove the AFF A700 controller module

Use the following procedure to remove the AFF A700 controller module.

Steps

- 1. Detach the console cable, if any, and the management cable from the controller module before removing the controller module.
- 2. Unlock and remove the controller module from the chassis.
 - a. Slide the orange button on the cam handle downward until it unlocks.



	Cam handle release button
	Cam handle

- b. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis. Make sure that you support the bottom of the controller module as you slide it out of the chassis.

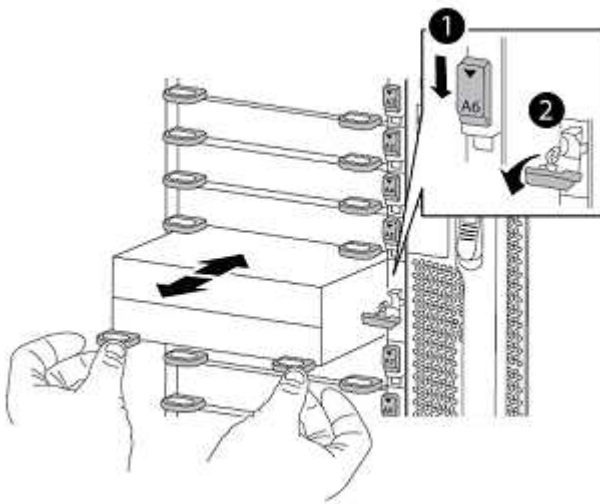
Remove the AFF A700 NVS module

Use the following procedure to remove the AFF A700 NVS module.



The AFF A700 NVS module is in slot 6 and is double the height compared to the other modules in the system.

1. Unlock and remove the NVS from slot 6.
 - a. Depress the lettered and numbered cam button. The cam button moves away from the chassis.
 - b. Rotate the cam latch down until it is in a horizontal position. The NVS disengages from the chassis and moves a few inches.
 - c. Remove the NVS from the chassis by pulling on the pull tabs on the sides of the module face.



	Lettered and numbered I/O cam latch
	I/O latch completely unlocked



If there are any add-on modules used as coredump devices on the AFF A700 non-volatile storage module, do not transfer those to the AFF A900 NVS. Do not transfer any parts from the AFF A700 controller module and NVS to the AFF A900.

Install the AFF A900 NVS and controller module

You must install the AFF A900 NVS and controller module from the upgrade kit on both nodes at Site_B. Do not move coredump device from AFF A700 NVS module to AFF A900 NVS module.

Before you start

If you are not already grounded, properly ground yourself.

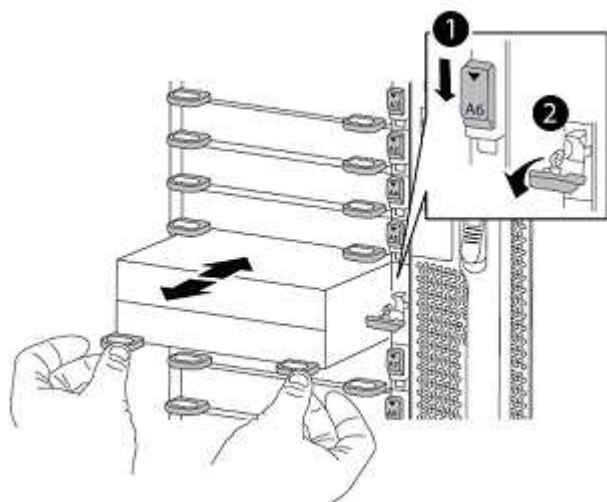
Install the AFF A900 NVS

Use the following procedure to install the AFF A900 NVS in slot 6 of both nodes at site_B

Steps

1. Align the NVS with the edges of the chassis opening in slot 6.
2. Gently slide the NVS into the slot until the lettered and numbered I/O cam latch begins to engage with the

I/O cam pin, and then push the I/O cam latch all the way up to lock the NVS in place.



	Lettered and numbered I/O cam latch
	I/O latch completely unlocked

Install the AFF A900 controller module

Use the following procedure to install the AFF A900 controller module.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Firmly push the controller module into the chassis until it meets the midplane and is fully seated. The locking latch rises when the controller module is fully seated.



Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

3. Cable the management and console ports to the controller module.



	Cam handle release button
	Cam handle

4. Install the second X91129A card in slot 7 of each node.
 - a. Connect FC-VI ports from slot 7 to the switches. Refer to the [Fabric-attached installation and configuration](#) documentation and go to the AFF A900 fabric MetroCluster connection requirements for the type of switch in your environment.
5. Power ON the chassis and connect to the serial console.
6. After BIOS initialization, if the node starts to autoboot, interrupt the AUTOBOOT by pressing Control-C.
7. After you interrupt the autoboot, the nodes stop at the LOADER prompt. If you do not interrupt autoboot on time and node1 starts booting, wait for the prompt to press Control-C to go into the boot menu. After the node stops at the boot menu, use option 8 to reboot the node and interrupt the autoboot during the reboot.
8. At the LOADER prompt, set the default environment variables: `set-defaults`
9. Save the default environment variables settings: `saveenv`

Netboot the nodes at site_B

After swapping the AFF A900 controller module and NVS, you need to netboot the AFF A900 nodes and install the same ONTAP version and patch level that is running on the cluster. The term `netboot` means you are booting from an ONTAP image stored on a remote server. When preparing for `netboot`, you must add a copy of the ONTAP 9 boot image onto a web server that the system can access.

It is not possible to check the ONTAP version installed on the boot media of an AFF A900 controller module unless it is installed in a chassis and powered ON. The ONTAP version on the AFF A900 boot media must be same as the ONTAP version running on the AFF A700 system that is being upgraded and both the primary and backup boot images should match. You can configure the images by performing a `netboot` followed by the `wipeconfig` command from the boot menu. If the controller module was previously used in another cluster, the `wipeconfig` command clears any residual configuration on the boot media.

Before you start

- Verify that you can access a HTTP server with the system.
- You need to download the necessary system files for your system and the correct version of ONTAP from the [NetApp Support](#) site. About this task You must `netboot` the new controllers if the version of ONTAP installed is not the same as the version installed on the original controllers. After you install each new controller, you boot the system from the ONTAP 9 image stored on the web server. You can then download the correct files to the boot media device for subsequent system boots.

Steps

1. Access [NetApp Support](#) to download the files required to perform a system netboot 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. Your directory listing should contain `<ontap_version>_image.tgz`.
4. Configure the `netboot` connection by choosing one of the following actions. Note: You should use the management port and IP as the `netboot` connection. Do not use a data LIF IP or a data outage might occur while the upgrade is being performed.

If Dynamic Host Configuration Protocol (DHCP) is...	Then...
Running	Configure the connection automatically by using the following command at the boot environment prompt: <code>ifconfig e0M -auto</code>
Not running	<p>Manually configure the connection by using the following command at the boot environment prompt: <code>ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> -dns=<dns_addr> domain=<dns_domain></code></p> <p><filer_addr> is the IP address of the storage system. <netmask> is the network mask of the storage system. <gateway> is the gateway for the storage system. <dns_addr> is the IP address of a name server on your network. This parameter is optional. <dns_domain> is the Domain Name Service (DNS) domain name. This parameter is optional.</p> <p>NOTE: Other parameters might be necessary for your interface. Enter <code>help ifconfig</code> at the firmware prompt for details.</p>

5. Perform `netboot` on node 1: `netboot http://<web_server_ip>/<path_to_web_accessible_directory>/netboot/kernel` The `<path_to_the_web_accessible_directory>` should lead to where you downloaded the `<ontap_version>_image.tgz` in [Step 2](#).



Do not interrupt the boot.

6. Wait for node 1 that is running on the AFF A900 controller module to boot and display the boot menu options as shown below:

Please choose one of the following:

- (1) Normal Boot.
 - (2) Boot without /etc/rc.
 - (3) Change password.
 - (4) Clean configuration and initialize all disks.
 - (5) Maintenance mode boot.
 - (6) Update flash from backup config.
 - (7) Install new software first.
 - (8) Reboot node.
 - (9) Configure Advanced Drive Partitioning.
 - (10) Set Onboard Key Manager recovery secrets.
 - (11) Configure node for external key management.
- Selection (1-11)?

7. From the boot menu, select option (7) Install new software first. This menu option downloads and installs the new ONTAP image to the boot device.



Disregard the following message: This procedure is not supported for Non-Disruptive Upgrade on an HA pair. This note applies to nondisruptive ONTAP software upgrades, and not controller upgrades. Always use netboot to update the new node to the desired image. If you use another method to install the image on the new controller, the wrong incorrect image might install. This issue applies to all ONTAP releases.

8. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL: http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
9. Complete the following substeps to reboot the controller module:
 - a. Enter `n` to skip the backup recovery when you see the following prompt: Do you want to restore the backup configuration now? {`y|n`}
 - b. Enter `y` to reboot when you see the following prompt: The node must be rebooted to start using the newly installed software. Do you want to reboot now? {`y|n`}

The controller module reboots but stops at the boot menu because the boot device was reformatted, and the configuration data needs to be restored.
10. At the prompt, run the `wipeconfig` command to clear any previous configuration on the boot media:
 - a. When you see the message below, answer `yes`: This will delete critical system configuration, including cluster membership. Warning: do not run this option on a HA node that has been taken over. Are you sure you want to continue?:
 - b. The node reboots to finish the `wipeconfig` and then stops at the boot menu.
11. Select option 5 to go to maintenance mode from the boot menu. Answer `yes` to the prompts until the node stops at maintenance mode and the command prompt `*>`.

Restore 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>

Set 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`.

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

```
ha-config modify controller mcc
```

```
ha-config modify chassis mcc
```

3. Halt the node: `halt` The node should stop at the `LOADER>` prompt.
4. On each node, check the system date, time, and time zone: `Show date`
5. If necessary, set the date in UTC or Greenwich Mean Time (GMT): `set date <mm/dd/yyyy>`
6. Check the time by using the following command at the boot environment prompt: `show time`
7. If necessary, set the time in UTC or GMT: `set time <hh:mm:ss>`
8. Save the settings: `saveenv`

9. Gather environment variables: `printenv`
10. Boot the node back into Maintenance mode to enable the configuration changes to take effect:
`boot_ontap maint`
11. Verify the changes you made are effective and `ucadmin` shows FC initiator ports online.

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

12. Verify the ha-config mode: `ha-config show`
 - a. Verify that you have the following output:

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

Set 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	<code>mcc-2n</code>
Four or eight nodes	<code>mcc</code>

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	<pre>ha-config modify controller mcc-2n ha-config modify chassis mcc-2n</pre>

Four or eight nodes	<pre>ha-config modify controller mcc ha-config modify chassis mcc</pre>
----------------------------	--

Reassign root aggregate disks

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

About this task

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-A700:

```
disk show -a
```

The example 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-A700(4068741254)	Pool1	PZHYN0MD	
	node_B_1-A700(4068741254)		node_B_1-A700(4068741254)	
rr18:9.126L49	node_B_1-A700(4068741254)	Pool1	PPG3J5HA	
	node_B_1-A700(4068741254)		node_B_1-A700(4068741254)	
rr18:8.126L21	node_B_1-A700(4068741254)	Pool1	PZHTDSZD	
	node_B_1-A700(4068741254)		node_B_1-A700(4068741254)	
rr18:8.126L2	node_B_1-A700(4068741254)	Pool0	S0M1J2CF	
	node_B_1-A700(4068741254)		node_B_1-A700(4068741254)	
rr18:8.126L3	node_B_1-A700(4068741254)	Pool0	S0M0CQM5	
	node_B_1-A700(4068741254)		node_B_1-A700(4068741254)	
rr18:9.126L27	node_B_1-A700(4068741254)	Pool0	S0M1PSDW	
	node_B_1-A700(4068741254)		node_B_1-A700(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
rr18:8.126L18	node_B_1-A900(1574774970)	Pool1	PZHYN0MD	
node_B_1-A900(1574774970)	node_B_1-A900(1574774970)			
rr18:9.126L49	node_B_1-A900(1574774970)	Pool1	PPG3J5HA	
node_B_1-A900(1574774970)	node_B_1-A900(1574774970)			
rr18:8.126L21	node_B_1-A900(1574774970)	Pool1	PZHTDSZD	
node_B_1-A900(1574774970)	node_B_1-A900(1574774970)			
rr18:8.126L2	node_B_1-A900(1574774970)	Pool0	S0M1J2CF	
node_B_1-A900(1574774970)	node_B_1-A900(1574774970)			
rr18:9.126L29	node_B_1-A900(1574774970)	Pool0	S0M0CQM5	
node_B_1-A900(1574774970)	node_B_1-A900(1574774970)			
rr18:8.126L1	node_B_1-A900(1574774970)	Pool0	S0M1PSDW	
node_B_1-A900(1574774970)	node_B_1-A900(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-A900).

Boot 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.

About this task

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...	Select this boot menu option...
Onboard key management	Option 10 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration
External key management	Option 11 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration

5. If autoboot is enabled, interrupt autoboot by pressing control-C.
6. From the boot menu, run option (6).



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 correct: `printenv partner-sysid`

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

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

If you are using...	Select this boot menu option...
Onboard key management	Option 10 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration
External key management	Option 11 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration

You might need to issue the `recover_XXXXXXX_keymanager` command at the boot menu prompt multiple times until the nodes completely 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.

[Add or remove 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	<pre>security key-manager onboard sync</pre> <p>For more information, see Restoring onboard key management encryption keys.</p>
External key management	<pre>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</pre> <p>For more information, see Restoring external key management encryption keys.</p>

Verify LIF configuration

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

About this task

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 vservice-name
```

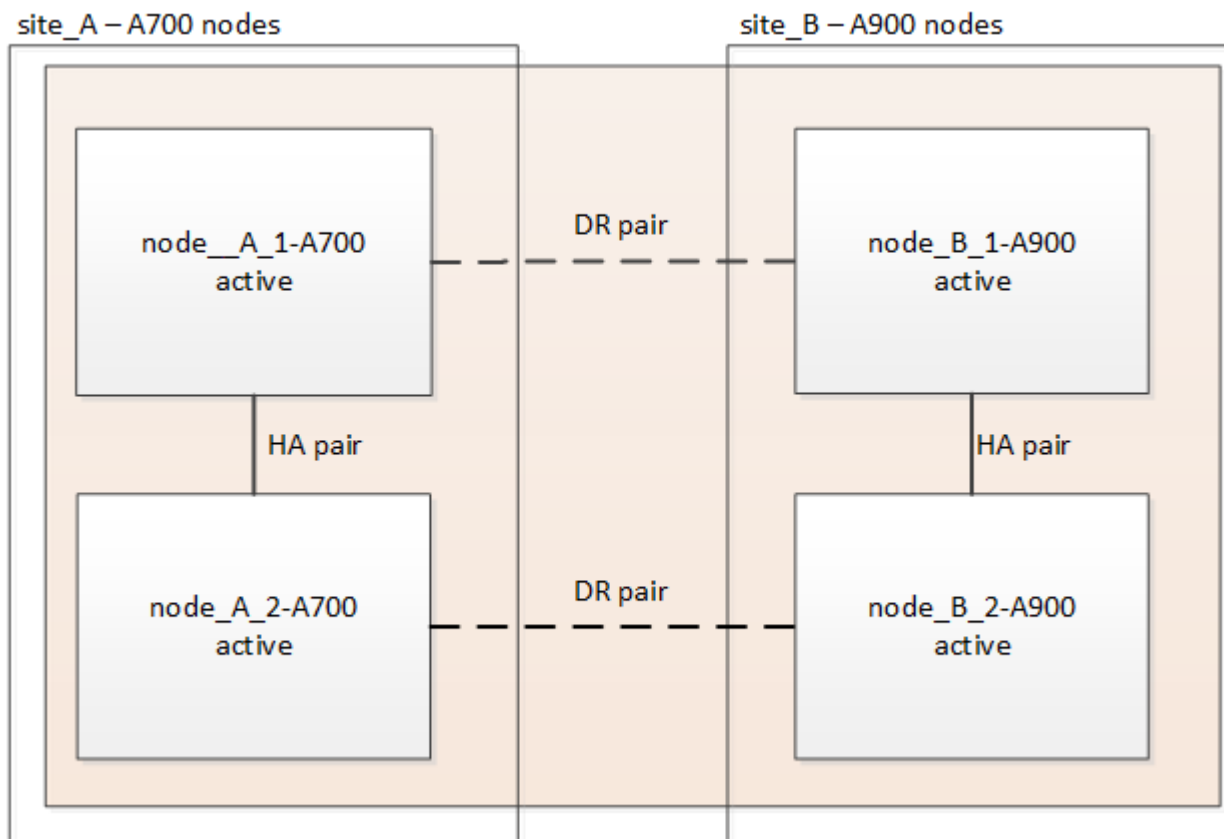
Perform this step on all SVMs as required.

Switch back the MetroCluster configuration

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

About this task

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.

Check the health of the MetroCluster configuration

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

About this task

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
```

Upgrade the nodes on site_A

You must repeat the upgrade tasks on site_A.

Step

1. Repeat the steps to upgrade the nodes on site_A, beginning with [Prepare for the upgrade](#).

As you perform the tasks, all example references to the sites and nodes are reversed. For example, when the example is given to switchover from site_A, you will switchover from Site_B.

Send 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.

Step

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.

Restore 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 [Add MetroCluster configurations](#) in the *MetroCluster Tiebreaker Installation and Configuration* section.

Upgrading controllers in a four-node MetroCluster FC configuration using switchover and switchback with "system controller replace" commands (ONTAP 9.10.1 and later)

You can use this guided automated MetroCluster switchover operation to perform a non-disruptive controller upgrade on a four-node MetroCluster FC configuration. Other components (such as storage shelves or switches) cannot be upgraded as part of this procedure.

About this task

- 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.

- This procedure applies to controller modules in a four-node MetroCluster FC configuration.
- The platforms must be running ONTAP 9.10.1 or later.
- Your original and new platforms must be compatible and supported.

The following table shows the supported model matrix for the controller upgrade.

Old platform model	Replacement platform model
AFF A300	AFF A400, AFF A700
FAS8200	FAS8300

NetApp Hardware Universe

- You can use this procedure to upgrade controllers in a four-node MetroCluster FC configuration using NSO based automated switchover and switchback. If you want to perform a controller upgrade using aggregate relocation (ARL), refer to [Use "system controller replace" commands to upgrade controller hardware running ONTAP 9.8 or later](#). It is recommended to use the NSO based automated procedure.
- If your MetroCluster sites are physically at two different locations, you should use the automated NSO controller upgrade procedure to upgrade the controllers at both sites in sequence.
- This automated NSO based controller upgrade procedure gives you the capability to initiate controller replacement to a MetroCluster disaster recovery (DR) site. You can only initiate a controller replacement at one site at a time.
- To initiate a controller replacement at site A, you need to run the controller replacement start command from site B. The operation guides you to replace controllers of both the nodes at site A only. To replace the controllers at site B, you need to run the controller replacement start command from site A. A message displays identifying the site at which the controllers are being replaced.

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

To prepare for the controller upgrade, you need to perform system prechecks and collect the configuration information.

At any stage during the upgrade, you can run the `system controller replace show` or `system controller replace show-details` command from site A to check the status. If the commands return a blank output, wait for a few minutes and rerun the command.

Steps

1. Start the automated controller replacement procedure from site A to replace the controllers at site B:

```
system controller replace start
```

The automated operation executes the prechecks. If no issues are found, the operation pauses so you can manually collect the configuration related information.



The current source system and all compatible target systems are displayed. If you have replaced the source controller with a controller that has a different ONTAP version or a non-compatible platform, the automation operation halts and reports an error after the new nodes are booted up. To bring the cluster back to a healthy state, you need to follow the manual recovery procedure.

The `system controller replace start` command might report the following precheck error:

```
Cluster-A::*>system controller replace show
Node           Status           Error-Action
-----
Node-A-1       Failed           MetroCluster check failed. Reason : MCC check
showed errors in component aggregates
```

Check if this error occurred because you have unmirrored aggregates or due to another aggregate issue. Verify that all mirrored aggregates are healthy and not degraded or mirror-degraded. If this error is due to unmirrored aggregates only, you can override this error by selecting the `-skip-metrocluster-check true` option on the `system controller replace start` command. If remote storage is accessible, the unmirrored aggregates come online after switchover. If the remote storage link fails, the unmirrored aggregates fail to come online.

2. Manually collect the configuration information by logging in at site B and following the commands listed in the console message under the `system controller replace show` or `system controller replace show-details` command.

Gathering information before the upgrade

Before upgrading, if the root volume is encrypted, you must gather the backup key and other information to boot the new controllers with the old encrypted root volumes.

About this task

This task is performed on the existing MetroCluster FC configuration.

Steps

1. Label the cables for the existing controllers, so you can easily identify the cables when setting up the new controllers.
2. Display the commands to capture the backup key and other information:

```
system controller replace show
```

Run the commands listed under the `show` command from the partner cluster.

3. 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.

4. 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

5. 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

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

```
security key-manager backup show
```

7. 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
```

8. After you finish collecting the configuration information, resume the operation:

```
system controller replace resume
```

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 replacing the old controller.

Steps

1. [Remove the existing MetroCluster configuration](#) from the Tiebreaker software.
2. Remove the existing MetroCluster configuration from any third-party application that can initiate switchover.

Refer to the documentation for the application.

Replacing the old controllers and booting up the new controllers

After you gather information and resume the operation, the automation proceeds with the switchover operation.

About this task

The automation operation initiates the switchover, `heal-aggregates`, and `heal root-aggregates` operations. After these operations complete, the operation pauses at **paused for user intervention** so you can rack and install the controllers, boot up the partner controllers and reassign the root aggregate disks to the new controller module from flash backup, using the `sysids` gathered earlier.

Before you begin

Before initiating switchover, the automation operation pauses so you can manually verify that all LIFs are “up” at site B. If necessary, bring any LIFs that are “down” to “up” and resume the automation operation by using the `system controller replace resume` command.

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.

About this task

- This task must be performed on each of the old nodes.
- You will use the information gathered in [Preparing for the upgrade](#).

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 the following 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 interface groups 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 elc-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
```

5. Halt the nodes:

```
halt -inhibit-takeover true -node node-name
```

This step must be performed on both nodes.

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.

Steps

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. Go 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 <code>ontap-version_image.tgz</code> file to the target directory: <code>tar -zxvf ontap-version_image.tgz</code></p> <p>NOTE: If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image.</p> <p>Your directory listing should contain a netboot folder with a kernel file: <code>netboot/kernel</code></p>
All other systems	<p>Your directory listing should contain a netboot folder with a kernel file: <code>ontap-version_image.tgz</code></p> <p>You do not need to extract the <code>ontap-version_image.tgz</code> file.</p>

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 the following 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}

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}

Clearing the configuration on a controller module

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

Steps

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
```

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.

- 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

- In Maintenance mode configure the settings for any HBAs in the system:
 - Check the current settings of the ports: `ucadmin show`
 - 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>

Reassigning root aggregate disks

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

About this task

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)	Pool11	PZHYN0MD	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:9.126L49	node_B_1-old(4068741254)	Pool11	PPG3J5HA	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:8.126L21	node_B_1-old(4068741254)	Pool11	PZHTDSZD	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:8.126L2	node_B_1-old(4068741254)	Pool10	S0M1J2CF	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:8.126L3	node_B_1-old(4068741254)	Pool10	S0M0CQM5	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:9.126L27	node_B_1-old(4068741254)	Pool10	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)   Pool11 PZHYN0MD
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool11 PPG3J5HA
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool11 PZHTDSZD
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool10 SOM1J2CF
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool10 SOM0CQM5
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool10 SOM1PSDW
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.

You can reconfigure VLANs and interface groups. If required, manually modify the ports for the cluster LIFs and broadcast domain details before resuming the operation by using the `system controller replace resume` command.

About this task

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, select the boot menu option for your key management configuration.

If you are using...	Select this boot menu option...
---------------------	---------------------------------

Onboard key management	Option “10” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.
External key management	Option “11” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.

5. If autoboot is enabled, interrupt autoboot by pressing Ctrl-C.
6. From the boot menu, run option “6”.



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 correct:

```
printenv partner-sysid
```

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

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

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

If you are using...	Select this boot menu option...
Onboard key management	Option “10” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.
External key management	Option “11” Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.

Depending on the key manager setting, perform the recovery procedure by selecting option “10” or option “11”, followed by option “6” at the first boot menu prompt. To boot the nodes completely, you might need to repeat the recovery procedure continued by option “1” (normal 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	<pre>security key-manager onboard sync</pre> <p>For more information, see Restoring onboard key management encryption keys.</p>
External key management	<pre>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</pre> <p>For more information, see Restoring external key management encryption keys.</p>

13. Before you resume the operation, verify that the MetroCluster is configured correctly. Check the node status:

```
metrocluster node show
```

Verify that the new nodes (site_B) are in **Waiting for switchback state** from site_A.

14. Resume the operation:

```
system controller replace resume
```

Completing the upgrade

The automation operation runs verification system checks and then pauses so you can verify the network reachability. After verification, the resource regain phase is initiated and the automation operation executes switchback at site A and pauses at the post upgrade checks. After you resume the automation operation, it performs the post upgrade checks and if no errors are detected, marks the upgrade as complete.

Steps

1. Verify the network reachability by following the console message.
2. After you complete the verification, resume the operation:

```
system controller replace resume
```

3. The automation operation performs switchback at site A and the post upgrade checks. When the operation pauses, manually check the SAN LIF status and verify the network configuration by following the console message.
4. After you complete the verification, resume the operation:

```
system controller replace resume
```

5. Check the post upgrade checks status:

```
system controller replace show
```

If the post upgrade checks did not report any errors, the upgrade is complete.

6. After you complete the controller upgrade, log in at site B and verify that the replaced controllers are configured correctly.

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](#).

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

Beginning 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.

About this task

- 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">• AFF A320	<ul style="list-style-type: none">• AFF A400
<ul style="list-style-type: none">• FAS8200	<ul style="list-style-type: none">• FAS9000• FAS8300• FAS8700



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.

About this task

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">AFF A400	<ul style="list-style-type: none">1020Any value in the range 101 to 4096 inclusive.

- 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.

Steps

- 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](#).

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

- Download and install the RCF files.

Follow the steps in the [MetroCluster IP installation and configuration](#).

- [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.

About this task

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						
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.

Steps

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:</p> <pre>tar -zxvf ontap-version_image.tgz</pre> <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> <pre>_ontap-version_image.tgz</pre> <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=<i>ip_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i></pre>

e. Perform the netboot.

If the platform model is...	Then...
FAS/AFF8000 series systems	<pre>netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel</pre>

All other systems	<pre>netboot http://_web_server_ip/path_to_web- accessible_directory/ontap- version_image.tgz</pre>
-------------------	---

- 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.

- g. 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
```

- h. Enter the user name and password if applicable, or press Enter to continue.
- i. 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**
```

- j. 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 existing configuration.

Steps

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
```

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 time zone 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 time zone.

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
- vservers 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:

- ° `fcg 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...
Tiebreaker	Removing MetroCluster Configurations in the <i>MetroCluster Tiebreaker Installation and Configuration Guide</i>
Mediator	Issue the following command from the ONTAP prompt: metrocluster configuration-settings mediator remove
Third-party applications	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.

About this task

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
```

The `maintenance-window-in-hours` parameter 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.

About this task

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.



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
```

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.

About this task

- 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 the following 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 elc-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.

About this task

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 procedure for your switch vendor:

[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 [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:

- Check the current settings of the ports:

```
ucadmin show
```

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

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	<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

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 “mccip”.

2. 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.

About this task

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
```

a. 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
```

b. 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.

About this task

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.

If you are using ADP...	Then use this command...
Yes	<code>disk reassign -s <i>old-sysid</i> -d <i>new-sysid</i> -r <i>dr-partner-sysid</i></code>
No	<code>disk reassign -s <i>old-sysid</i> -d <i>new-sysid</i></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	OWNER	POOL	SERIAL NUMBER
HOME	DR HOME		
prod03-rk18:8.126L18	node_B_1-new(537097247)	Pool1	PZHYN0MD
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod04-rk18:9.126L49	node_B_1-new(537097247)	Pool1	PPG3J5HA
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod04-rk18:8.126L21	node_B_1-new(537097247)	Pool1	PZHTDSZD
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod02-rk18:8.126L2	node_B_1-new(537097247)	Pool0	S0M1J2CF
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod02-rk18:9.126L29	node_B_1-new(537097247)	Pool0	S0M0CQM5
node_B_1-new(537097247)	node_B_1-new(537097247)		
prod01-rk18:8.126L1	node_B_1-new(537097247)	Pool0	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, select the boot menu option for your key management configuration.

If you are using...	Select this boot menu option...
Onboard key management	Option 10 Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.
External key management	Option 11 Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.

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, select the boot menu option again for your key management configuration.

If you are using...	Select this boot menu option...
Onboard key management	Option 10 Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.
External key management	Option "11" Follow the prompts to provide the required inputs to recover and restore the key-manager configuration.

Depending on the key manager setting, perform the recovery procedure by selecting option "10" or option "11", followed by option 6 at the first boot menu prompt. To boot the nodes completely, you might need to repeat the recovery procedure continued by option "1" (normal 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 Restoring onboard key management encryption keys .
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 Restoring external key management encryption keys .

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.

About this task

- 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
```

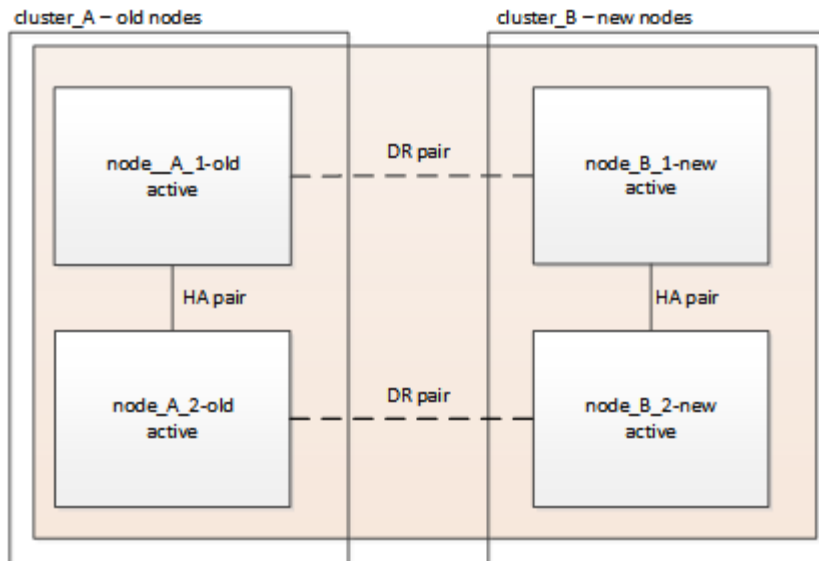
2. Revert the interfaces to their home node:

```
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.

About this task

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
Tiebreaker	Adding MetroCluster configurations .
Mediator	Configuring the ONTAP Mediator service from a MetroCluster IP configuration .
Third-party applications	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.

Upgrade controllers from AFF A700 to AFF A900 in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.10.1 and later)

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.

About this task

- The controllers must be running ONTAP 9.10.1 or later.
- This procedure applies to AFF A700 controller modules upgrading to an AFF A900 in a MetroCluster IP configuration.

Old platform model	New platform model
• AFF A700	• AFF A900

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

Operating the MetroCluster configuration with an AFF A700 and an AFF A900 controller is not supported outside of this maintenance activity.

- The IP switches must be running a supported firmware version.
- 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-A700
- node_A_2-A700

- After upgrade:

- node_A_1-A900
- node_A_2-A900

- Site_B

- Before upgrade:

- node_B_1-A700
- node_B_2-A700

- After upgrade:

- node_B_1-A900
- node_B_2-A900

Workflow for upgrading controllers in a MetroCluster IP configuration

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



Prepare 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.

Clear slot 7 on the AFF A700 controller

The MetroCluster configuration on an AFF A900 uses one of each of the ports on the DR cards located in slots 5 and 7. Before starting the upgrade, if there are cards in slot 7 on the AFF A700, you must move them to other slots for all the nodes of the cluster.

Update the MetroCluster switch RCF files before upgrading controllers

The MetroCluster IP configuration on an AFF A700 does not use VLANs. The MetroCluster configuration on an AFF A900 does use VLANs. As a result, you need to change the RCF file when upgrading from an AFF A700 to an AFF A900.

Platform model	Supported VLAN IDs
<ul style="list-style-type: none">AFF A900	<ul style="list-style-type: none">1020Any value in the range 101 to 4096 inclusive.

- If the switch is not configured with the minimum supported RCF file version, you must update the RCF file. For the correct RCF file version for your switch model, refer to the [RcfFileGenerator Tool](#). The following steps are for the RCF file application.

Steps

- 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](#) content.

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

- Download and install the RCF files.

Follow the steps in the [MetroCluster IP Installation and Configuration](#) content.

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

Map ports from the old nodes to the new nodes

When upgrading from an AFF A700 to an AFF A900, you do not change the data network ports, FCP SAN adapter ports, and SAS and NVMe storage ports. Data LIFs stay where they are during and after the upgrade. Therefore, you are not required to map the network ports from the old nodes to the new nodes.

Verify MetroCluster health before site upgrade

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

Steps

- Verify the operation of the MetroCluster configuration in ONTAP:

- 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.

- 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 time zone 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` command to configure the time and time zone.

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.

Gather 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 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-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1          cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1          cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1          cluster_B node_B_2-A700 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-A700	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2-A700	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1-A700	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2-A700	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:

- ° 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
```

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-A700  537403324    537403323
537403321    537403322
1            cluster_A node_A_2-A700  537403323    537403324
537403322    537403321
1            cluster_B node_B_1-A700  537403322    537403321
537403323    537403324
1            cluster_B node_B_2-A700  537403321    537403322
537403324    537403323
4 entries were displayed.
```

Remove 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...
---------------------	-----------------------

Tiebreaker	Removing MetroCluster Configurations in the <i>MetroCluster Tiebreaker Installation and Configuration content</i>
Mediator	Issue the following command from the ONTAP prompt: metrocluster configuration-settings mediator remove
Third-party applications	Refer to the product documentation.

Send a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify 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.

About this task

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
```

The `maintenance-window-in-hours` parameter 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.

Switch over the MetroCluster configuration

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

About this task

This task must be performed on site_A.

After completing this task, site_A is active and serving data for both sites. site_B is inactive, and ready to begin the upgrade process.



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 site_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. Nodes at site_B are halted and stopped at the `LOADER` prompt.

Remove AFF A700 platform controller module and NVS

About this task

If you are not already grounded, properly ground yourself.

Steps

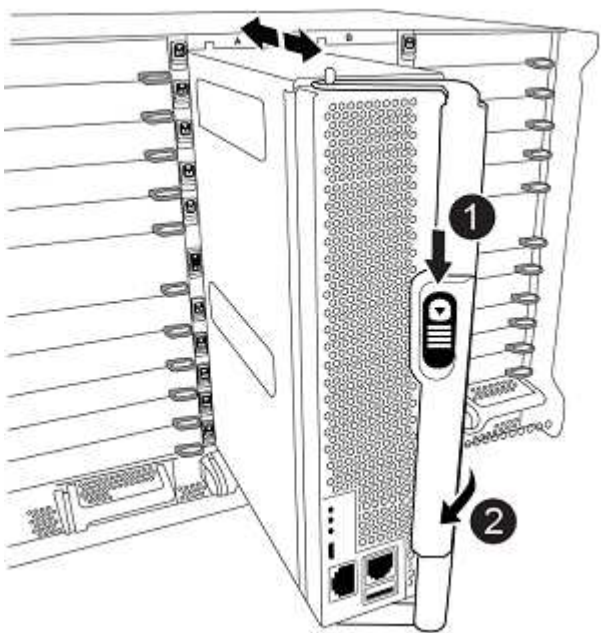
- 1. Gather the bootarg values from both nodes at site_B: `printenv`
- 2. Power off the chassis at site_B.



Remove the AFF A700 controller module

Use the following procedure to remove the AFF A700 controller module

Steps

- 1. Detach the console cable, if any, and the management cable from the controller module before removing the controller module.
- 2. Unlock and remove the controller module from the chassis.
 - a. Slide the orange button on the cam handle downward until it unlocks.



	Cam handle release button
	Cam handle

- b. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis. Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Remove the AFF A700 NVS module

Use the following procedure to remove the AFF A700 NVS module.

Note: The AFF A700 NVS module NVS module is in slot 6 and is double the height compared to other modules in the system.

Steps

1. Unlock and remove the NVS from slot 6.
 - a. Depress the lettered and numbered 'cam' button. The cam button moves away from the chassis.
 - b. Rotate the cam latch down until it is in a horizontal position. The NVS disengages from the chassis and moves a few inches.
 - c. Remove the NVS from the chassis by pulling on the pull tabs on the sides of the module face.



	Lettered and numbered I/O cam latch
	I/O latch completely unlocked

2. If you are using add-on modules used as coredump devices on the AFF A700 NVS, do not transfer them to the AFF A900 NVS. Do not transfer any parts from the AFF A700 controller module and NVS to the AFF A900.

Install the AFF A900 NVS and controller modules

You must install the AFF A900 NVS and controller module that you received in the upgrade kit on both nodes at site_B. Do not move the coredump device from the AFF A700 NVS module to the AFF A900 NVS module.

About this task

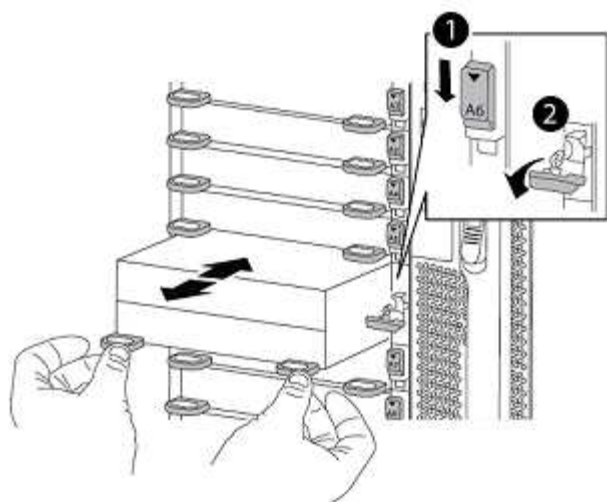
If you are not already grounded, properly ground yourself.

Install the AFF A900 NVS

Use the following procedure to install the AFF A900 NVS in slot 6 of both nodes at site_B.

Steps

1. Align the NVS with the edges of the chassis opening in slot 6.
2. Gently slide the NVS into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the NVS in place.



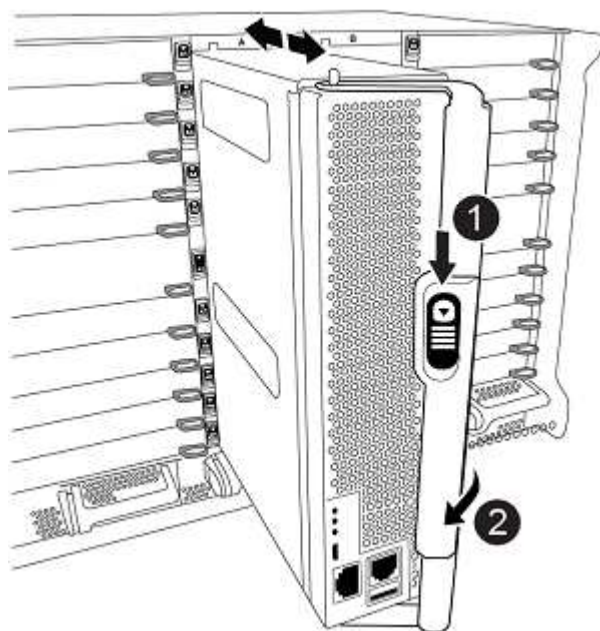
	Lettered and numbered I/O cam latch
	I/O latch completely unlocked



Install the AFF A900 controller module.

Use the following procedure to install the AFF A900 controller module.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Firmly push the controller module into the chassis until it meets the midplane and is fully seated. The locking latch rises when the controller module is fully seated. Attention: To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.
3. Cable the management and console ports to the controller module.



	Cam handle release button
	Cam handle

4. Install the second X91146A card in slot 7 of each node.

- a. Move the e5b connection to e7b.
- b. Move the e5a connection to e5b.



Slot 7 on all nodes of the cluster should be empty as mentioned in [Map ports from the old nodes to the new nodes](#) section.

5. Power ON the chassis and connect to serial console.
6. After BIOS initialization, if the node starts autoboot, interrupt the AUTOBOOT by pressing Control-C.
7. After autoboot is interrupted, the nodes stop at the LOADER prompt. If you do not interrupt autoboot on time and node1 starts booting, wait for the prompt to press Ctrl-C to go into the boot menu. After the node stops at the boot menu, use option 8 to reboot the node and interrupt the autoboot during reboot.
8. At the LOADER prompt, set the default environment variables: `set-defaults`
9. Save the default environment variables settings: `saveenv`

Netboot nodes at site_B

After swapping the AFF A900 controller module and NVS, you need to netboot the AFF A900 nodes and install the same ONTAP version and patch level that is running on the cluster. The term netboot means you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you must add a copy of the ONTAP 9 boot image onto a web server that the system can access. It is not possible to check the version of ONTAP installed on the boot media of an AFF A900 controller module unless it is installed in a chassis and powered ON. The ONTAP version on the AFF A900 boot media must be the same as the ONTAP version running on the AFF A700 system that is being upgraded and both the primary and backup boot images should match. You can configure the images by performing a netboot followed by the `wipeconfig` command from the boot menu. If the controller module was previously used in another cluster, the `wipeconfig` command clears any residual configuration on the boot media.

Before you start

- Verify that you can access a HTTP server with the system.
- You need to download the necessary system files for your system and the correct version of ONTAP from the NetApp Support Site.

About this task

You must netboot the new controllers, if the version of ONTAP installed is not the same as the version installed on the original controllers. After you install each new controller, you boot the system from the ONTAP 9 image stored on the web server. You can then download the correct files to the boot media device for subsequent system boots.

Steps

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.
4. Your directory listing should contain <ontap_version>_image.tgz.
5. Configure the netboot connection by choosing one of the following actions.



You should use the management port and IP as the netboot connection. Do not use a data LIF IP or a data outage might occur while the upgrade is being performed.

If the Dynamic Host Configuration Protocol (DHCP) is...	Then...
Running	Configure the connection automatically by using the following command at the boot environment prompt: <code>ifconfig e0M -auto</code>
Not Running	Manually configure the connection by using the following command at the boot environment prompt: <code>ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain></code> <filer_addr> is the IP address of the storage system. <netmask> is the network mask of the storage system. <gateway> is the gateway for the storage system. <dns_addr> is the IP address of a name server on your network. This parameter is optional. <dns_domain> is the Domain Name Service (DNS) domain name. This parameter is optional. NOTE: Other parameters might be necessary for your interface. Enter <code>help ifconfig</code> at the firmware prompt for details.

6. Perform netboot on node_B_1: `netboot http://<web_server_ip/<path_to_web_accessible_directory>/netboot/kernel`

The <path_to_the_web-accessible_directory> should lead to where you downloaded the <ontap_version>_image.tgz in [Step 2](#).



Do not interrupt the boot.

7. Wait for the node_B_1 now running on the AFF A900 controller module to boot and display the boot menu options as shown below:

Please choose one of the following:

- (1) Normal Boot.
 - (2) Boot without /etc/rc.
 - (3) Change password.
 - (4) Clean configuration and initialize all disks.
 - (5) Maintenance mode boot.
 - (6) Update flash from backup config.
 - (7) Install new software first.
 - (8) Reboot node.
 - (9) Configure Advanced Drive Partitioning.
 - (10) Set Onboard Key Manager recovery secrets.
 - (11) Configure node for external key management.
- Selection (1-11)?

8. From the boot menu, select option (7) Install new software first. This menu option downloads and installs the new ONTAP image to the boot device. **NOTE:** Disregard the following message: This procedure is not supported for Non-Disruptive Upgrade on an HA pair. This note applies to nondisruptive ONTAP software upgrades, and not controller upgrades.

Always use netboot to update the new node to the desired image. If you use another method to install the image on the new controller, the incorrect image might install. This issue applies to all ONTAP releases.

9. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL: `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`
10. Complete the following substeps to reboot the controller module:
- a. Enter `n` to skip the backup recovery when you see the following prompt: Do you want to restore the backup configuration now? {y|n}
 - b. Enter `y` to reboot when you see the following prompt: `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n} The controller module reboots but stops at the boot menu because the boot device was reformatted, and the configuration data needs to be restored.
11. At the prompt, run the `wipeconfig` command to clear any previous configuration on the boot media:
- a. When you see the following message, answer `yes`: This will delete critical system configuration, including cluster membership. Warning: do not run this option on a HA node that has been taken over. Are you sure you want to continue?:
 - b. The node reboots to finish the `wipeconfig` and then stops at the boot menu.
12. Select option 5 to go to maintenance mode from the boot menu. Answer `yes` to the prompts until the node stops at maintenance mode and the command prompt `*>`.
13. Repeat these steps to netboot node_B_2.

Restore 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>

- 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	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

Set 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 `mccip`.

2. 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
```

3. Halt the node: `halt`

The node should stop at the `LOADER>` prompt.

4. On each node, check the system date, time, and time zone: `show date`
5. If necessary, set the date in UTC or GMT: `set date <mm/dd/yyyy>`
6. Check the time by using the following command at the boot environment prompt: `show time`
7. If necessary, set the time in UTC or GMT: `set time <hh:mm:ss>`
8. Save the settings: `saveenv`
9. Gather environment variables: `printenv`

Update the switch RCF files to accommodate the new platforms

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

About this task

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* section.

[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](#)

Configure the new controllers

New controllers should be ready and cabled at this point.

Set 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.

About this task

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. At the `LOADER>` prompt, set the following bootargs on the new nodes at site_B:

```
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
```

The following example sets the values for node_B_1-A900 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 example sets the values for node_B_2-A900 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
```

2. 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
```


- a. Set the UUIDs on node_B_1-A900.

The following example shows the commands for setting the UUIDs on node_B_1-A900:

```
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
```

- b. Set the UUIDs on node_B_2-A900:

The following example shows the commands for setting the UUIDs on node_B_2-A900:

```
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
```

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

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

4. 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-A700.

- a. Set the variables on node_B_1-A900.

The following example shows the commands for setting the values on node_B_1-A900:

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

- b. Set the variables on node_B_2-A900.

The following example shows the commands for setting the values on node_B_2-A900:

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

5. 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
```

Reassign root aggregate disks

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

About this task

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-A900 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-A700(537403322)  Pool11  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool11  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21  node_B_1-A700(537403322)  Pool11  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2   node_B_1-A700(537403322)  Pool10  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3   node_B_1-A700(537403322)  Pool10  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27  node_B_1-A700(537403322)  Pool10  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.

```

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

If you are using ADP...	Then use this command...
Yes	<code>disk reassign -s <i>old-sysid</i> -d <i>new-sysid</i> -r <i>dr-partner-sysid</i></code>
No	<code>disk reassign -s <i>old-sysid</i> -d <i>new-sysid</i></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 correctly 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-A900 (537097247)	Pool1	PZHYN0MD
node_B_1-A900 (537097247)	node_B_1-A900 (537097247)		
prod04-rk18:9.126L49	node_B_1-A900 (537097247)	Pool1	PPG3J5HA
node_B_1-A900 (537097247)	node_B_1-A900 (537097247)		
prod04-rk18:8.126L21	node_B_1-A900 (537097247)	Pool1	PZHTDSZD
node_B_1-A900 (537097247)	node_B_1-A900 (537097247)		
prod02-rk18:8.126L2	node_B_1-A900 (537097247)	Pool0	S0M1J2CF
node_B_1-A900 (537097247)	node_B_1-A900 (537097247)		
prod02-rk18:9.126L29	node_B_1-A900 (537097247)	Pool0	S0M0CQM5
node_B_1-A900 (537097247)	node_B_1-A900 (537097247)		
prod01-rk18:8.126L1	node_B_1-A900 (537097247)	Pool0	S0M1PSDW
node_B_1-A900 (537097247)	node_B_1-A900 (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	

Boot 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, select the boot menu option for your key management configuration.

If you are using...	Select this boot menu option...
Onboard key management	Option 10 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration
External key management	Option 11 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration

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. Interrupt the AUTOBOOT to stop the controllers at LOADER.



On each node, check the bootargs set in [Setting the MetroCluster IP bootarg variables](#) and correct any incorrect values. Only move to the next step after you have checked the bootarg values.

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, select the boot menu option for your key management configuration.

If you are using...	Select this boot menu option...
Onboard key management	Option 10 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration
External key management	Option 11 and follow the prompts to provide the required inputs to recover or restore the key-manager configuration

You need to perform the recovery procedure by selecting Option 10 or option 11 depending on the key manager setting and Option 6 at the boot menu prompt. To boot the nodes completely, you might need to perform the recovery procedure continued by option 1 (normal boot).

10. Wait for the new nodes, node_B_1-A900 and node_B_2-A900 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 Restoring onboard key management encryption keys .
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 Restoring external key management encryption keys .

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](#)

Verify and restore LIF configuration

Verify that LIFs are hosted on appropriate nodes and ports as mapped out at the beginning of the upgrade procedure.

About this task

- 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.

Switch 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 from 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.

Check the health of the MetroCluster configuration

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

About this task

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
```

Upgrade the nodes on site_A

You must repeat the upgrade tasks on site_A.

Steps

1. Repeat the steps to upgrade the nodes on site_A, beginning with [Prepare for the upgrade](#).

As you perform the tasks, all example references to the sites and nodes are reversed. For example, when the example is given to switchover from site_A, you will switchover from site_B.

Restore 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
Tiebreaker	Adding MetroCluster configurations in the <i>MetroCluster Tiebreaker Installation and Configuration</i> section.
Mediator	Configuring the ONTAP Mediator service from a MetroCluster IP configuration in the <i>MetroCluster IP Installation and Configuration</i> section.
Third-party applications	Refer to the product documentation.

Send 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.

Refreshing a four-node MetroCluster FC configuration

You can upgrade the controllers and storage in a four-node MetroCluster configuration by expanding the configuration to become an eight-node configuration and then removing the old disaster recovery (DR) group.

About this task

References to "old nodes" mean the nodes that you intend to replace.

Steps

1. Gather information from the old nodes.

At this stage, the four-node configuration appears as shown in the following image:



2. Perform all of the steps in the four-node expansion procedure for your MetroCluster type.

[Expanding a four-node MetroCluster FC configuration to an eight-node configuration](#)

When the expansion procedure is complete, the configuration appears as shown in the following image:



3. Move the CRS volumes.

Perform the steps in [Moving a metadata volume in MetroCluster configurations](#).

4. Move the data from the old nodes to new nodes using the following procedures from [Other platform procedures: Controller Hardware Upgrade Express](#).

- a. Perform all the steps in [Creating an aggregate and moving volumes to the new nodes](#).



You might choose to mirror the aggregate when or after it is created.

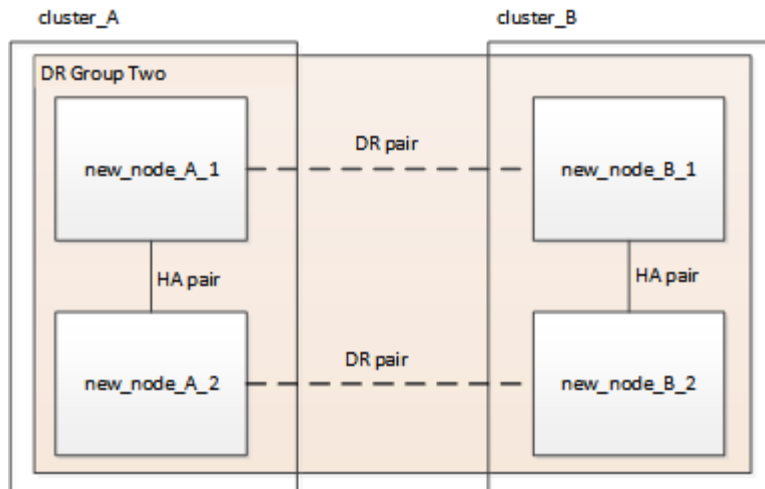
- b. Perform all the steps in [Moving non-SAN data LIFs and cluster management LIFs to the new nodes](#).

- c. Perform all the steps in [Deleting SAN LIFs from the original nodes](#).

5. Follow the steps in the procedure for removing the old DR group.

[Removing a Disaster Recovery group](#)

After you have removed the old DR group (DR group one), the configuration appears as shown in the following image:



Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Beginning with ONTAP 9.8, you can upgrade the controllers and storage in a four-node MetroCluster IP configuration by expanding the configuration to become a temporary eight-node configuration and then removing the old disaster recovery (DR) group.

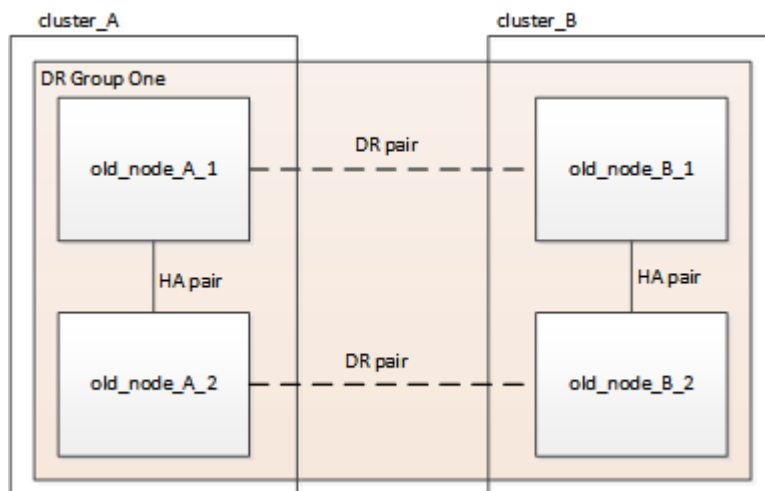
About this task

- This procedure is supported on systems running ONTAP 9.8 and later.
- If you are upgrading the IP switches, they should be upgraded before performing this refresh procedure.
- References to "old nodes" mean the nodes that you intend to replace.
- This procedure is not supported on AFF A320 systems configured with Broadcom BES-53248 switches.

Steps

1. Gather information from the old nodes.

At this stage, the four-node configuration appears as shown in the following image:



2. To prevent automatic support case generation, send an AutoSupport message to indicate the upgrade is

underway.

- a. Issue the following command:

```
system node autosupport invoke -node * -type all -message "MAINT=10h  
Upgrading old-model to new-model"
```

The following example specifies a 10 hour maintenance window. You might want to allow additional time depending on your plan.

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.

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

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

4. Perform all of the steps in [Expanding a four-node MetroCluster IP configuration to an eight-node configuration](#) to add the new nodes and storage to the configuration.

When the expansion procedure is complete, the configuration appears as shown in the following image:



5. Move the CRS volumes.

Perform the steps in [Moving a metadata volume in MetroCluster configurations](#).

6. Move the data from the old nodes to new nodes using the following procedures in [Other platform procedures: Controller Hardware Upgrade Express Guide](#)
 - a. Perform all the steps in [Creating an aggregate and moving volumes to the new nodes](#).



You might choose to mirror the aggregate when or after it is created.

- b. Perform all the steps in [Moving non-SAN data LIFs and cluster management LIFs to the new nodes](#).
7. Follow the steps in the procedure for removing the old DR group.

[Removing a Disaster Recovery group](#)

After you have removed the old DR group (DR group one), the configuration appears as shown in the following image:



8. 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
```

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

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

10. 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.

Expand a two-node MetroCluster FC configuration to a four-node configuration

Expanding a two-node MetroCluster FC configuration to a four-node configuration

Expanding a two-node MetroCluster FC configuration to a four-node MetroCluster FC configuration involves adding a controller to each cluster to form an HA pair at each MetroCluster site, and then refreshing the MetroCluster FC configuration.

Before you begin

- The nodes must be running ONTAP 9 or later in a MetroCluster FC configuration.

This procedure is not supported on earlier versions of ONTAP or in MetroCluster IP configurations.

- If the platforms in your two-node configuration are not supported in ONTAP 9.2 and you plan to upgrade to platforms supported in ONTAP 9.2 *and* expand to a four-node cluster, you must upgrade the platforms in the two-node configuration *before* expanding the MetroCluster FC configuration.
- The existing MetroCluster FC configuration must be healthy.
- The equipment you are adding must be supported and meet all of the requirements described in the following procedures:

[Fabric-attached MetroCluster installation and configuration](#)

[Stretch MetroCluster installation and configuration](#)

- You must have available FC switch ports to accommodate the new controllers and any new bridges.
- You need the admin password and access to an FTP or SCP server.

About this task

- This procedure applies only to MetroCluster FC configurations.
- This procedure is disruptive and takes approximately four hours to complete.
- Before performing this procedure, the MetroCluster FC configuration consists of two single-node clusters:



After completing this procedure, the MetroCluster FC configuration consists of two HA pairs, one at each site:



- Both sites must be expanded equally.

A MetroCluster configuration cannot consist of an uneven number of nodes.

- This procedure can take over an hour per site, with additional time for tasks such as initializing the disks and netbooting the new nodes.

The time to initialize the disks depends on the size of the disks.

- This procedure uses the following workflow:



Verifying the state of the MetroCluster configuration

You should identify the existing controllers and confirm the disaster recovery (DR)

relationships between them, that the controllers are in normal mode, and that the aggregates are mirrored.

Steps

- 1. Display the details of the nodes in the MetroCluster configuration from any node in the configuration:

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

The following output shows that this MetroCluster configuration has a single DR group and one node in each cluster.

```
cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
systemid

dr-group-id  cluster          node              dr-partner        dr-partner-
systemid
-----
1            cluster_A       controller_A_1    controller_B_1    536946192
1            cluster_B       controller_B_1    controller_A_1    536946165
2 entries were displayed.
```

- 2. Display the state of the MetroCluster configuration:

```
metrocluster show
```

The following output shows that the existing nodes in the MetroCluster configuration are in normal mode:

```
cluster_A::> metrocluster show

Configuration: two-node-fabric

Cluster          Entry Name          State
-----
Local: cluster_A  Configuration State configured
                  Mode          normal
                  AUSO Failure Domain auso-on-cluster-
disaster
Remote: controller_B_1_siteB
                  Configuration State configured
                  Mode          normal
                  AUSO Failure Domain auso-on-cluster-
disaster
```

- 3. Check the state of the aggregates on each node in the MetroCluster configuration:

```
storage aggregate show
```

The following output shows that the aggregates on cluster_A are online and mirrored:

```
cluster_A::> storage aggregate show
```

Aggregate RAID Status	Size	Available	Used%	State	#Vols	Nodes
-----	-----	-----	-----	-----	-----	-----
aggr0_controller_A_1_0	1.38TB	68.63GB	95%	online	1	
controller_A_1 raid_dp,mirrored						
controller_A_1_aggr1	4.15TB	4.14TB	0%	online	2	
controller_A_1 raid_dp,mirrored						
controller_A_1_aggr2	4.15TB	4.14TB	0%	online	1	
controller_A_1 raid_dp,mirrored						

3 entries were displayed.

```
cluster_A::>
```

Sending a custom AutoSupport message before adding nodes to the MetroCluster configuration

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.

About this task

This task must be performed on each MetroCluster site.

Steps

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

```
system node autosupport invoke -node * -type all -message MAINT=maintenance-  
window-in-hours
```

The `maintenance-window-in-hours` parameter specifies the length of the maintenance window and can be a maximum of 72 hours. If you complete the maintenance before the time has elapsed, you can issue the following command to indicate that the maintenance period has ended:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Repeat this step on the partner site.

Zoning for the new controller ports when adding a controller module in a fabric-attached MetroCluster configuration

The FC switch zoning must accommodate the new controller connections. If you used the NetApp-supplied reference configuration files (RCFs) to configure your switches, the zoning is preconfigured and you do not need to make any changes.

If you manually configured your FC switches, you must ensure that the zoning is correct for the initiator connections from the new controller modules. See the sections on zoning in [Fabric-attached MetroCluster installation and configuration](#).

Add a new controller module to each cluster

Adding a new controller module to each cluster

You must add a new controller module to each site, creating an HA pair in each site. This is a multistep process involving both hardware and software changes that must be performed in the proper order at each site.

About this task

- The new controller module must be received from NetApp as part of the upgrade kit.

You should verify that PCIe cards in the new controller module are compatible and supported by the new controller module.

[NetApp Hardware Universe](#)

- Your system must have an empty slot available for the new controller module when upgrading to a single-chassis HA pair (an HA pair in which both controller modules reside in the same chassis).



This configuration is not supported on all systems. Platforms with single chassis configurations that are supported in ONTAP 9 are AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx, FAS8020, FAS8060, FAS8080, and FAS9000.

- You must have rack space and cables for the new controller module when upgrading to a dual-chassis HA pair (an HA pair in which the controller modules reside in separate chassis).



This configuration is not supported on all systems.

- You must connect each controller module to the management network through its e0a port or, if your system has one, you can connect to the e0M port as the management port.
- These tasks must be repeated at each site.
- The preexisting controller modules are referred to as the *existing* controller modules.

The examples in this procedure have the console prompt `existing_ctlr>`.

- The controller modules that are being added are referred to as the *new* controller modules; the examples in this procedure have the console prompt `new_ctlr>`.
- This task uses the following workflow:



Preparing for the upgrade

Before upgrading to an HA pair, you must verify that your system meets all requirements and that you have all of the necessary information.

Steps

1. You need to identify unassigned disks or spare disks that you can assign to the new controller module.

[Physical Storage Management](#)

[Disk and aggregate management](#)

2. Based on the results of the previous step, perform either of the following:

If the result showed...	Then...
-------------------------	---------

Not enough spare disks available for the new controller module on a system without root-data partitioning	Contact technical support for more information.
Other results	<p>Complete the following substeps:</p> <p>a. Determine where the aggregates for the existing node are located:</p> <pre>storage aggregate show</pre> <p>b. If disk ownership automatic assignment is on, turn it off:</p> <pre>storage disk option modify -node <i>node_name</i> -autoassign off</pre> <p>c. Remove ownership on disks that do not have aggregates on them:</p> <pre>storage disk removeowner <i>disk_name</i></pre> <p>d. Repeat the previous step for as many disks as you need for the new node.</p>

3. Verify that you have cables ready for the following connections:

- Cluster connections

If you are creating a two-node switchless cluster, you require two cables to connect the controller modules. Otherwise, you require a minimum of four cables, two for each controller module connection to the cluster-network switch. Other systems (like the 80xx series) have defaults of either four or six cluster connections.

- HA interconnect connections, if the system is in a dual-chassis HA pair

4. Verify that you have a serial port console available for the controller modules.

5. Verify that your environment meets the site and system requirements.

[NetApp Hardware Universe](#)

6. Gather all of the IP addresses and other network parameters for the new controller module.

Clearing the configuration on a controller module

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

Steps

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
```

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.

Preparing cluster ports on an existing controller module

Before installing a new controller module, you must configure cluster ports on the existing controller module so that the cluster ports can provide cluster communication with the new controller module.

About this task

If you are creating a two-node switchless cluster (with no cluster network switches), you must enable the switchless cluster networking mode.

For detailed information about port, LIF, and network configuration in ONTAP, see [Network Management](#).

Steps

1. Determine which ports should be used as the node's cluster ports.

For a list of the default port roles for your platform, see the [Hardware Universe](#)

The *Installation and Setup Instructions* for your platform on the NetApp Support Site contains information about the ports for cluster network connections.

2. For each cluster port, identify the port roles:

```
network port show
```

In the following example, ports “e0a”, “e0b”, “e0c”, and “e0d” must be changed to cluster ports:

```
cluster_A::> network port show
```

```
Node: controller_A_1
```

```
Speed(Mbps) Health
```

Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
e0M	Default	mgmt_bd_1500	up	1500	auto/1000	healthy
e0a	Default	Default	up	1500	auto/10000	healthy
e0b	Default	Default	up	1500	auto/10000	healthy
e0c	Default	Default	up	1500	auto/10000	healthy
e0d	Default	Default	up	1500	auto/10000	healthy
e0i	Default	Default	down	1500	auto/10	-
e0j	Default	Default	down	1500	auto/10	-
e0k	Default	Default	down	1500	auto/10	-
e0l	Default	Default	down	1500	auto/10	-
e2a	Default	Default	up	1500	auto/10000	healthy
e2b	Default	Default	up	1500	auto/10000	healthy
e4a	Default	Default	up	1500	auto/10000	healthy
e4b	Default	Default	up	1500	auto/10000	healthy

```
13 entries were displayed.
```

3. For any data LIF that is using a cluster port as the home-port or current-port, modify the LIF to use a data port as its home-port:

```
network interface modify
```

The following example changes the home port of a data LIF to a data port:

```
cluster1::> network interface modify -lif datalif1 -vserver vs1 -home  
-port e1b
```

4. For each LIF that you modified, revert the LIF to its new home port:

```
network interface revert
```

The following example reverts the LIF “datalif1” to its new home port “e1b”:

```
cluster1::> network interface revert -lif datalif1 -vserver vs1
```

5. 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 elc-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
```

6. Verify that the port roles have changed:

```
network port show
```

The following example shows that ports “e0a”, “e0b”, “e0c”, and “e0d” are now cluster ports:

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
-----
e0M       Default      mgmt_bd_1500    up    1500    auto/1000  healthy
e0a       Cluster      Cluster         up    9000    auto/10000 healthy
e0b       Cluster      Cluster         up    9000    auto/10000 healthy
e0c       Cluster      Cluster         up    9000    auto/10000 healthy
e0d       Cluster      Cluster         up    9000    auto/10000 healthy
e0i       Default      Default         down  1500    auto/10    -
e0j       Default      Default         down  1500    auto/10    -
e0k       Default      Default         down  1500    auto/10    -
e0l       Default      Default         down  1500    auto/10    -
e2a       Default      Default         up    1500    auto/10000 healthy
e2b       Default      Default         up    1500    auto/10000 healthy
e4a       Default      Default         up    1500    auto/10000 healthy
e4b       Default      Default         up    1500    auto/10000 healthy
13 entries were displayed.
```

7. Add the ports to the cluster broadcast domain:

```
broadcast-domain add-ports -ipSpace Cluster -broadcast-domain Cluster -ports  
port-id, port-id, port-id...
```

For example:

```
broadcast-domain add-ports -ipSpace Cluster -broadcast-domain Cluster  
-ports cluster1-01:e0a
```

8. If your system is part of a switched cluster, create cluster LIFs on the cluster ports: `network interface create`

The following example creates a cluster LIF on one of the node's cluster ports. The `-auto` parameter configures the LIF to use a link-local IP address.

```
cluster1::> network interface create -vserver Cluster -lif clus1 -role  
cluster -home-node node0 -home-port e1a -auto true
```

9. If you are creating a two-node switchless cluster, enable the switchless cluster networking mode:

a. Change to the advanced privilege level from either node:

```
set -privilege advanced
```

You can respond `y` when prompted whether you want to continue into advanced mode. The advanced mode prompt appears (`*>`).

b. Enable the switchless cluster networking mode:

```
network options switchless-cluster modify -enabled true
```

c. Return to the admin privilege level:

```
set -privilege admin
```



Cluster interface creation for the existing node in a two-node switchless cluster system is completed after cluster setup is completed through a netboot on the new controller module.

Preparing the netboot server to download the image

When you are ready to prepare the netboot server, you must download the correct ONTAP netboot image from the NetApp Support Site to the netboot server and note the IP address.

About this task

- You must be able to access an HTTP server from the system before and after adding the new controller module.

- You must have access to the NetApp Support Site to download the necessary system files for your platform and your version of ONTAP.

[NetApp Support Site](#)

- Both controller modules in the HA pair must run the same version of ONTAP.

Steps

1. 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.

The `<ontap_version>_image.tgz` file is used for performing a netboot of your system.

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

For...	Then...
FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 series systems	<p>Extract the contents of the <code><ontap_version>_image.tgz</code> file to the target directory:</p> <pre>tar -zxvf <ontap_version>_image.tgz</pre> <div>  <p>If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image.</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 the following file:</p> <pre><ontap_version>_image.tgz</pre> <div>  <p>There is no need to extract the file contents.</p> </div>

3. Determine the IP address of the existing controller module.

This address is referred to later in this procedure as *ip-address-of-existing controller*.

4. Ping *ip-address-of-existing controller* to verify that the IP address is reachable.

Setting the HA mode on the existing controller module

You must use the storage failover modify command to set the mode on the existing controller module. The mode value is enabled later, after you reboot the controller module.

Steps

- 1. Set the mode to HA:

```
storage failover modify -mode ha -node existing_node_name
```

Shutting down the existing controller module

You must perform a clean shutdown of the existing controller module to verify that all of the data has been written to disk. You must also disconnect the power supplies.

About this task



You must perform a clean system shutdown before replacing the system components to avoid losing unwritten data in the NVRAM or NVMEM.

Steps

- 1. Halt the node from the existing controller module prompt:

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

If you are prompted to continue the halt procedure, enter *y* when prompted, and then wait until the system stops at the LOADER prompt.

In an 80xx system, the NVRAM LED is located on the controller module to the right of the network ports, marked with a battery symbol.

This LED blinks if there is unwritten data in the NVRAM. If this LED is flashing amber after you enter the halt command, you need to reboot your system and try halting it again.

- 2. If you are not already grounded, properly ground yourself.
- 3. Turn off the power supplies and disconnect the power, using the correct method for your system and power-supply type:

If your system uses...	Then...
AC power supplies	Unplug the power cords from the power source, and then remove the power cords.
DC power supplies	Remove the power at the DC source, and then remove the DC wires, if necessary.

Install and cable the new controller module

Installing and cabling the new controller module

You must physically install the new controller module in the chassis, and then cable it.

Steps

- 1. If you have an I/O expansion module (IOXM) in your system and are creating a single-chassis HA pair, you must uncable and remove the IOXM.

You can then use the empty bay for the new controller module. However, the new configuration will not have the extra I/O provided by the IOXM.

2. Physically install the new controller module and, if necessary, install additional fans:

If you are adding a controller module...	Then perform these steps...
To an empty bay to create a single-chassis HA pair and the system belongs to one of the following platforms:	<ol style="list-style-type: none"> a. Remove the blank plate in the rear of the chassis that covers the empty bay that will contain the new controller module. b. Gently push the controller module halfway into the chassis. <p>To prevent the controller module from automatically booting, do not fully seat it in the chassis until later in this procedure.</p>
<p>In a separate chassis from its HA partner to create a dual-chassis HA pair when the existing configuration is in a controller-IOX module configuration.</p> <ul style="list-style-type: none"> • FAS8200 • 80xx 	Install the new system in the rack or system cabinet.

3. Cable the cluster network connections, as necessary:

- a. Identify the ports on the controller module for the cluster connections.

[AFF A320 systems: Installation and setup](#)

[AFF A220/FAS2700 Systems Installation and Setup Instructions](#)

[AFF A800 Systems Installation and Setup Instructions](#)

[AFF A300 Systems Installation and Setup Instructions](#)

[FAS8200 Systems Installation and Setup Instructions](#)

- b. If you are configuring a switched cluster, identify the ports that you will use on the cluster network switches.

See the *Clustered Data ONTAP Switch Setup Guide for Cisco Switches*, *NetApp 10G Cluster-Mode Switch Installation Guide* or *NetApp 1G Cluster-Mode Switch Installation Guide*, depending on what switches you are using.

- c. Connect cables to the cluster ports:

If the cluster is...	Then...
----------------------	---------

A two-node switchless cluster	Directly connect the cluster ports on the existing controller module to the corresponding cluster ports on the new controller module.
A switched cluster	Connect the cluster ports on each controller to the ports on the cluster network switches identified in Substep b.

Cabling the new controller module's FC-VI and HBA ports to the FC switches

The new controller module's FC-VI ports and HBAs (host bus adapters) must be cabled to the site FC switches.

Steps

1. Cable the FC-VI ports and HBA ports, using the table for your configuration and switch model.
 - [Port assignments for FC switches when using ONTAP 9.1 and later](#)
 - [Port assignments for FC switches when using ONTAP 9.0](#)
 - [Port assignments for systems using two initiator ports](#)

Cabling the new controller module's cluster peering connections

You must cable the new controller module to the cluster peering network so that it has connectivity with the cluster on the partner site.

About this task

At least two ports on each controller module should be used for cluster peering.

The recommended minimum bandwidth for the ports and network connectivity is 1 GbE.

Steps

1. Identify and cable at least two ports for cluster peering and verify they have network connectivity with the partner cluster.

Powering up both controller modules and displaying the LOADER prompt

You power up the existing controller module and the new controller module to display the LOADER prompt.

Steps

Power up the controller modules and interrupt the boot process, using the steps for your configuration:

If the controller modules are...	Then...
----------------------------------	---------

In the same chassis	<p>a. Verify that the new controller module is not fully inserted into the bay.</p> <p>The existing controller module should be fully inserted into the bay because it was never removed from the chassis, but the new controller module should not be.</p> <p>b. Connect the power and turn on the power supplies so that the existing controller module receives power.</p> <p>c. Interrupt the boot process on the existing controller module by pressing Ctrl-C.</p> <p>d. Push the new controller module firmly into the bay.</p> <p>When fully seated, the new controller module receives power and automatically boots.</p> <p>e. Interrupt the boot process by pressing Ctrl-C.</p> <p>f. Tighten the thumbscrew on the cam handle, if present.</p> <p>g. Install the cable management device, if present.</p> <p>h. Bind the cables to the cable management device with the hook and loop strap.</p>
In separate chassis	<p>a. Turn on the power supplies on the existing controller module.</p> <p>b. Interrupt the boot process by pressing Ctrl-C.</p> <p>c. Repeat these steps for the new controller module</p>

Each controller module should display the LOADER prompt (LOADER>, LOADER-A>, or LOADER-B>).



If there is no LOADER prompt, record the error message and contact technical support. If the system displays the boot menu, reboot and attempt to interrupt the boot process again.

Changing the ha-config setting on the existing and new controller modules

When you expand a MetroCluster configuration, you must update the ha-config setting of the existing controller module and the new controller module. You must also determine the system ID of the new controller module.

About this task

This task is performed in Maintenance mode on both the existing and new controller modules.

Steps

1. Change the ha-config setting of the existing controller module:
 - a. Display the ha-config setting of the existing controller module and chassis:

```
ha-config show
```

The ha-config setting is “mcc-2n” for all components because the controller module was in a two-node MetroCluster configuration.

- b. Change the ha-config setting of the existing controller module to "mcc":

```
ha-config modify controller mcc
```

- c. Change the ha-config setting of the existing chassis to "mcc":

```
ha-config modify chassis mcc
```

- d. Retrieve the system ID for the existing controller module:

```
sysconfig
```

Note the system ID. You need it when you set the partner ID on the new controller module.

- e. Exit Maintenance mode to return to the LOADER prompt:

```
halt
```

2. Change the ha-config setting and retrieve the system ID of the new controller module:

- a. If the new controller module is not already in Maintenance mode, boot it to Maintenance mode:

```
boot_ontap maint
```

- b. Change the ha-config setting of the new controller module to "mcc":

```
ha-config modify controller mcc
```

- c. Change the ha-config setting of the new chassis to mcc:

```
ha-config modify chassis mcc
```

- d. Retrieve the system ID for the new controller module:

```
sysconfig
```

Note the system ID. You need it when you set the partner ID and assign disks to the new controller module.

- e. Exit Maintenance mode to return to the LOADER prompt:

```
halt
```

Setting the partner system ID for both controller modules

You must set the partner system ID on both controller modules so that they can form an HA pair.

About this task

This task is performed with both controller modules at the LOADER prompt.

Steps

1. On the existing controller module, set the partner system ID to that of the new controller module:

```
setenv partner-sysid sysID_of_new_controller
```

2. On the new controller module, set the partner system ID to that of the existing controller module:

```
setenv partner-sysid sysID_of_existing_controller
```

Booting the existing controller module

You must boot the existing controller module to ONTAP.

Steps

1. At the LOADER prompt, boot the existing controller module to ONTAP:

```
boot_ontap
```

Assigning disks to the new controller module

Before you complete the configuration of the new controller module through netboot, you must assign disks to it.

About this task

You must have made sure that there are enough spares, unassigned disks, or assigned disks that are not part of an existing aggregate.

Preparing for the upgrade

These steps are performed on the existing controller module.

Steps

1. Assign the root disk to the new controller module:

```
storage disk assign -disk disk_name -sysid new_controller_sysID -force true
```

If your platform model uses the Advanced Drive Partitioning (ADP) feature, you must include the `-root true` parameter:

```
storage disk assign -disk disk_name -root true -sysid new_controller_sysID -force true
```

2. Assign the remaining required disks to the new controller module by entering the following command for each disk:

```
storage disk assign -disk disk_name -sysid new_controller_sysID -force true
```

3. Verify that the disk assignments are correct:

```
storage disk show -partitionownership*
```



Ensure that you have assigned all disks that you intend to assign to the new node.

Netbooting and setting up ONTAP on the new controller module

You must perform a specific sequence of steps to netboot and install the ONTAP operating system on the new controller module when adding controller modules to an existing MetroCluster configuration.

About this task

- This task starts at the LOADER prompt of the new controller module.
- This task includes initializing disks.

The amount of time you need to initialize the disks depends on the size of the disks.

- The system automatically assigns two disks to the new controller module.

[Disk and aggregate management](#)

Steps

1. At the LOADER prompt, configure the IP address of the new controller module based on DHCP availability:

If DHCP is...	Then enter the following command...
Available	ifconfig e0M -auto
Not available	<pre>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></pre> <p><i>filer_addr</i> is the IP address of the storage system.</p> <p><i>netmask</i> is the network mask of the storage system.</p> <p><i>gateway</i> is the gateway for the storage system.</p> <p><i>dns_addr</i> is the IP address of a name server on your network.</p> <p><i>dns_domain</i> is the Domain Name System (DNS) domain name. If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL; you need only the server's host name.</p> <div> Other parameters might be necessary for your interface. For details, use the <code>help ifconfig</code> command at the LOADER prompt.</div>

2. At the LOADER prompt, netboot the new node:

For...	Issue this command...
--------	-----------------------

FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 series systems	netboot http://web_server_ip/path_to_web- accessible_directory/netboot/kernel
All other systems	netboot http://web_server_ip/path_to_web- accessible_directory/<ontap_version>_image.tgz

The `path_to_the_web-accessible_directory` is the location of the downloaded `<ontap_version>_image.tgz` file.

3. Select the **Install new software first** option from the displayed menu.

This menu option downloads and installs the new ONTAP image to the boot device.

- You should enter “y” when prompted with the message that this procedure is not supported for nondisruptive upgrade on an HA pair.
- You should enter “y” when warned that this process replaces the existing ONTAP software with new software.
- You should enter the path as follows when prompted for the URL of the image.tgz file:

```
http://path_to_the_web-accessible_directory/image.tgz
```

4. Enter “y” when prompted regarding nondisruptive upgrade or replacement of the software.

5. Enter the path to the image.tgz file when prompted for the URL of the package.

```
What is the URL for the package? `http://path_to_web-
accessible_directory/image.tgz`
```

6. Enter “n” to skip the backup recovery when prompted to restore the backup configuration.

```
*****
*               Restore Backup Configuration               *
* This procedure only applies to storage controllers that  *
* are configured as an HA pair.                            *
*                                                         *
* Choose Yes to restore the "varfs" backup configuration  *
* from the SSH server. Refer to the Boot Device Replacement *
* guide for more details.                                  *
* Choose No to skip the backup recovery and return to the *
* boot menu.                                               *
*****

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

7. Enter “y” when prompted to reboot now.

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

8. If necessary, select the option to **Clean configuration and initialize all disks** after the node has booted.

Because you are configuring a new controller module and the new controller module’s disks are empty, you can respond “y” when the system warns you that this will erase all disks.



The amount of time needed to initialize disks depends on the size of your disks and configuration.

9. After the disks are initialized and the Cluster Setup wizard starts, set up the node:

Enter the node management LIF information on the console.

10. Log in to the node, and enter the `cluster setup` and then enter “join” when prompted to join the cluster.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}: `join`
```

11. Respond to the remaining prompts as appropriate for your site.

The [Setup ONTAP](#) for your version of ONTAP contains additional details.

12. If the system is in a two-node switchless cluster configuration, create the cluster interfaces on the existing node using the network interface create command to create cluster LIFs on the cluster ports.

The following is an example command for creating a cluster LIF on one of the node’s cluster ports. The `-auto` parameter configures the LIF to use a link-local IP address.

```
cluster_A::> network interface create -vserver Cluster -lif clus1 -role
cluster -home-node node_A_1 -home-port e1a -auto true
```

13. After setup is complete, verify that the node is healthy and eligible to participate in the cluster:

```
cluster show
```

The following example shows a cluster after the second node (cluster1-02) has been joined to it:

```
cluster_A::> cluster show
Node           Health Eligibility
-----
node_A_1       true  true
node_A_2       true  true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin storage virtual machine (SVM) or node SVM by using the cluster setup command.

14. Confirm that you have four ports configured as cluster interconnects:

```
network port show
```

The following example shows output for two controller modules in cluster_A:

```
cluster_A::> network port show
```

							Speed
(Mbps)							
Node	Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----	

node_A_1							
	**e0a	Cluster	Cluster		up	9000	
	auto/1000						
	e0b	Cluster	Cluster		up	9000	
	auto/1000**						
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000
	e0e	Default	Default		up	1500	auto/1000
	e0f	Default	Default		up	1500	auto/1000
	e0g	Default	Default		up	1500	auto/1000
node_A_2							
	**e0a	Cluster	Cluster		up	9000	
	auto/1000						
	e0b	Cluster	Cluster		up	9000	
	auto/1000**						
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000
	e0e	Default	Default		up	1500	auto/1000
	e0f	Default	Default		up	1500	auto/1000
	e0g	Default	Default		up	1500	auto/1000

14 entries were displayed.

Mirroring the root aggregate on the new controller

You must mirror the root aggregate to provide data protection when you are adding a controller to a MetroCluster configuration.

This task must be performed on the new controller module.

1. Mirror the root aggregate:

```
storage aggregate mirror aggr_name
```

The following command mirrors the root aggregate for controller_A_1:

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

This mirrors the aggregate, so it consists of a local plex and a remote plex located at the remote MetroCluster site.

Configure intercluster LIFs

Configuring intercluster LIFs on dedicated ports

You can configure intercluster LIFs on dedicated ports. Doing so typically increases the available bandwidth for replication traffic.

Steps

1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

The following example shows the network ports in cluster01:


```
cluster01::> network port show
```

(Mbps)		Speed				
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper

cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000

2. Determine which ports are available to dedicate to intercluster communication:

```
network interface show -fields home-port,curr-port
```

For complete command syntax, see the man page.

The following example shows that ports "e0e" and "e0f" have not been assigned LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1 e0a      e0a
Cluster cluster01-01_clus2 e0b      e0b
Cluster cluster01-02_clus1 e0a      e0a
Cluster cluster01-02_clus2 e0b      e0b
cluster01
    cluster_mgmt            e0c      e0c
cluster01
    cluster01-01_mgmt1      e0c      e0c
cluster01
    cluster01-02_mgmt1      e0c      e0c
```

3. Create a failover group for the dedicated ports:

network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical_or_logical_ports

The following example assigns ports "e0e" and "e0f" to the failover group "intercluster01" on the system SVM "cluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

network interface failover-groups show

For complete command syntax, see the man page.

```
cluster01::> network interface failover-groups show
Vserver      Group      Failover
-----
Targets
-----
Cluster
Cluster
cluster01-01:e0a, cluster01-01:e0b,
cluster01-02:e0a, cluster01-02:e0b
cluster01
Default
cluster01-01:e0c, cluster01-01:e0d,
cluster01-02:e0c, cluster01-02:e0d,
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
intercluster01
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
```

5. Create intercluster LIFs on the system SVM and assign them to the failover group.

ONTAP version	Command
9.6 and later	network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group

9.5 and earlier	<pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group</pre>
-----------------	---

For complete command syntax, see the man page.

The following example creates intercluster LIFs "cluster01_icl01" and "cluster01_icl02" in the failover group "intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
<pre>network interface show -service-policy default-intercluster</pre>
In ONTAP 9.5 and earlier:
<pre>network interface show -role intercluster</pre>

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0e
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0f
true				

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster -failover
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster -failover
```

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs "cluster01_icl01" and "cluster01_icl02" on the SVM "e0e" port will fail over to the "e0f" port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical	Home	Failover	Failover
	Interface	Node:Port	Policy	Group
cluster01	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01			Failover Targets: cluster01-01:e0e, cluster01-01:e0f	
	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01			Failover Targets: cluster01-02:e0e, cluster01-02:e0f	

Configuring intercluster LIFs on shared data ports

You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

Steps

- 1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

The following example shows the network ports in cluster01:

```
cluster01::> network port show
```

(Mbps)					Speed	
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper

cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000

- 2. Create intercluster LIFs on the system SVM:

In ONTAP 9.6 and later:
<pre>network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask</pre>
In ONTAP 9.5 and earlier:
<pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask</pre>

For complete command syntax, see the man page.

The following example creates intercluster LIFs cluster01_icl01 and cluster01_icl02:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster
```

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-intercluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	

cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01	e0c
true					
	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02	e0c
true					

4. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster -failover
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster -failover
```

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs "cluster01_icl01" and "cluster01_icl02" on the "e0c" port will fail over to the "e0d" port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-01:e0c, cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-02:e0c, cluster01-02:e0d	

Creating a mirrored data aggregate on each node

You must create a mirrored data aggregate on each node in the DR group.

About this task

- You should know what drives will be used in the new aggregate.
- If you have multiple drive types in your system (heterogeneous storage), you should understand how you can ensure that the correct drive type is selected.
- Drives are owned by a specific node; when you create an aggregate, all drives in that aggregate must be owned by the same node, which becomes the home node for that aggregate.

In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions.

- Aggregate names should conform to the naming scheme you determined when you planned your MetroCluster configuration.

[Disk and aggregate management](#)

Steps

1. Display a list of available spares:

```
storage disk show -spare -owner node_name
```

2. Create the aggregate:

```
storage aggregate create -mirror true
```

If you are logged in to the cluster on the cluster management interface, you can create an aggregate on any node in the cluster. To ensure that the aggregate is created on a specific node, use the `-node` parameter or specify drives that are owned by that node.

You can specify the following options:

- Aggregate's home node (that is, the node that owns the aggregate in normal operation)
- List of specific drives that are to be added to the aggregate
- Number of drives to include



In the minimum supported configuration, in which a limited number of drives are available, you must use the `force-small-aggregate` option to allow the creation of a three disk RAID-DP aggregate.

- Checksum style to use for the aggregate
- Type of drives to use
- Size of drives to use
- Drive speed to use
- RAID type for RAID groups on the aggregate
- Maximum number of drives that can be included in a RAID group
- Whether drives with different RPM are allowed

For more information about these options, see the `storage aggregate create` man page.

The following command creates a mirrored aggregate with 10 disks:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10
-node node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verify the RAID group and drives of your new aggregate:

```
storage aggregate show-status -aggregate aggregate-name
```

Installing licenses for the new controller module

You must add licenses for the new controller module for any ONTAP services that require standard (node-locked) licenses. For features with standard licenses, each node in the cluster must have its own key for the feature.

For detailed information about licensing, see the knowledgebase article 3013749: Data ONTAP 8.2 Licensing

Overview and References on the NetApp Support Site and the *System Administration Reference*.

Steps

1. If necessary, obtain license keys for the new node on the NetApp Support Site in the My Support section under Software licenses.

If the site does not have the license keys you need, contact your sales or support representative.

2. Issue the following command to install each license key:

```
system license add -license-code license_key
```

The *license_key* is 28 digits in length.

3. Repeat this step for each required standard (node-locked) license.

Creating unmirrored data aggregates

You can optionally create unmirrored data aggregates for data that does not require the redundant mirroring provided by MetroCluster configurations.

About this task

- You should know what drives or array LUNs will be used in the new aggregate.
- If you have multiple drive types in your system (heterogeneous storage), you should understand how you can verify that the correct drive type is selected.



In MetroCluster IP configurations, remote unmirrored aggregates are not accessible after a switchover



The unmirrored aggregates must be local to the node owning them.

- Drives and array LUNs are owned by a specific node; when you create an aggregate, all drives in that aggregate must be owned by the same node, which becomes the home node for that aggregate.
- Aggregate names should conform to the naming scheme you determined when you planned your MetroCluster configuration.
- *Disks and aggregates management* contains more information about mirroring aggregates.

Steps

1. Enable unmirrored aggregate deployment:

```
metrocluster modify -enable-unmirrored-aggr-deployment true
```

2. Verify that disk auto-assignment is disabled:

```
disk option show
```

3. Install and cable the disk shelves that will contain the unmirrored aggregates.

You can use the procedures in the *Installation and Setup* documentation for your platform and disk shelves.

[AFF and FAS Documentation Center](#)

4. Manually assign all disks on the new shelf to the appropriate node:

```
disk assign -disk disk-id -owner owner-node-name
```

5. Create the aggregate:

```
storage aggregate create
```

If you are logged in to the cluster on the cluster management interface, you can create an aggregate on any node in the cluster. To verify that the aggregate is created on a specific node, you should use the `-node` parameter or specify drives that are owned by that node.

You must also ensure that you are only including drives on the unmirrored shelf to the aggregate.

You can specify the following options:

- Aggregate's home node (that is, the node that owns the aggregate in normal operation)
- List of specific drives or array LUNs that are to be added to the aggregate
- Number of drives to include
- Checksum style to use for the aggregate
- Type of drives to use
- Size of drives to use
- Drive speed to use
- RAID type for RAID groups on the aggregate
- Maximum number of drives or array LUNs that can be included in a RAID group
- Whether drives with different RPM are allowed

For more information about these options, see the `storage aggregate create` man page.

The following command creates a unmirrored aggregate with 10 disks:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

6. Verify the RAID group and drives of your new aggregate:

```
storage aggregate show-status -aggregate aggregate-name
```

7. Disable unmirrored aggregate deployment:

```
metrocluster modify -enable-unmirrored-aggr-deployment false
```

8. Verify that disk auto-assignment is enabled:

```
disk option show
```

Related information

[Disk and aggregate management](#)

Installing the firmware after adding a controller module

After adding the controller module, you must install the latest firmware on the new controller module so that the controller module functions properly with ONTAP.

Steps

1. Download the most current version of firmware for your system and follow the instructions for downloading and installing the new firmware.

[NetApp Downloads: System Firmware and Diagnostics](#)

Refreshing the MetroCluster configuration with new controllers

You must refresh the MetroCluster configuration when expanding it from a two-node configuration to a four-node configuration.

Steps

1. Refresh the MetroCluster configuration:
 - a. Enter advanced privilege mode:
`set -privilege advanced`
 - b. Refresh the MetroCluster configuration:
`metrocluster configure -refresh true -allow-with-one-aggregate true`

The following command refreshes the MetroCluster configuration on all of the nodes in the DR group that contains controller_A_1:

```
controller_A_1::*> metrocluster configure -refresh true -allow-with  
-one-aggregate true  
  
[Job 726] Job succeeded: Configure is successful.
```

- c. Return to admin privilege mode:

```
set -privilege admin
```

2. Verify the networking status on site A:

```
network port show
```

The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper

controller_A_1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
controller_A_2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

```
14 entries were displayed.
```

3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.

a. Verify the configuration from site A:

```
metrocluster show
```

```
cluster_A::> metrocluster show
```

Cluster	Entry Name	State

Local: cluster_A	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		
Remote: cluster_B	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		

b. Verify the configuration from site B:

```
metrocluster show
```

```
cluster_B::> metrocluster show
```

Cluster	Entry Name	State
-----	-----	-----
Local: cluster_B	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		
Remote: cluster_A	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		

c. Verify that the DR relationships have been created correctly:

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner
```

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner
```

dr-group-id	cluster	node	ha-partner	dr-cluster	dr-partner
dr-auxiliary	node-object-limit	automatic-uso			
-----	-----	---	-----	-----	-----
2	cluster_A	node_A_1	node_A_2	cluster_B	node_B_1
node_B_2	on		true		
2	cluster_A	node_A_2	node_A_1	cluster_B	node_B_2
node_B_1	on		true		
2	cluster_B	node_B_1	node_B_2	cluster_A	node_A_1
node_A_2	on		true		
2	cluster_B	node_B_2	node_B_1	cluster_A	node_A_2
node_A_1	on		true		

4 entries were displayed.

Enabling storage failover on both controller modules and enabling cluster HA

After adding new controller modules to the MetroCluster configuration, you must enable storage failover on both controller modules and separately enable cluster HA.

Before you begin

The MetroCluster configuration must have previously been refreshed using the `metrocluster configure -refresh true` command.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Enable storage failover:

```
storage failover modify -enabled true -node existing-node-name
```

The single command enables storage failover on both controller modules.

2. Verify that storage failover is enabled:

```
storage failover show
```

The output should be similar to the following:

Node	Partner	Possible	State Description
old-ctlr	new-ctlr	true	Connected to new-ctlr
new-ctlr	old-ctlr	true	Connected to old-ctlr
2 entries were displayed.			

3. Enable cluster HA:

```
cluster ha modify -configured true
```

Cluster high availability (HA) must be configured in a cluster if it contains only two nodes and it differs from the HA provided by storage failover.

Restarting the SVMs

After expanding the MetroCluster configuration, you must restart the SVMs.

Steps

1. Identify the SVMs that need to be restarted:

```
metrocluster vserver show
```

This command shows the SVMs on both MetroCluster clusters.

2. Restart the SVMs on the first cluster:

- a. Enter advanced privilege mode, pressing **y** when prompted:

```
set -privilege advanced
```

- b. Restart the SVMs:

```
vserver start -vserver SVM_name -force true
```

- c. Return to admin privilege mode:

```
set -privilege admin
```

3. Repeat the previous step on the partner cluster.
4. Verify that the SVMs are in a healthy state:

```
metrocluster vserver show
```

Expand a four-node MetroCluster FC configuration to an eight-node configuration

Expanding a four-node MetroCluster FC configuration to an eight-node configuration

Expanding a four-node MetroCluster FC configuration to an eight-node MetroCluster FC configuration involves adding two controllers to each cluster to form a second HA pair at each MetroCluster site, and then running the MetroCluster FC configuration operation.

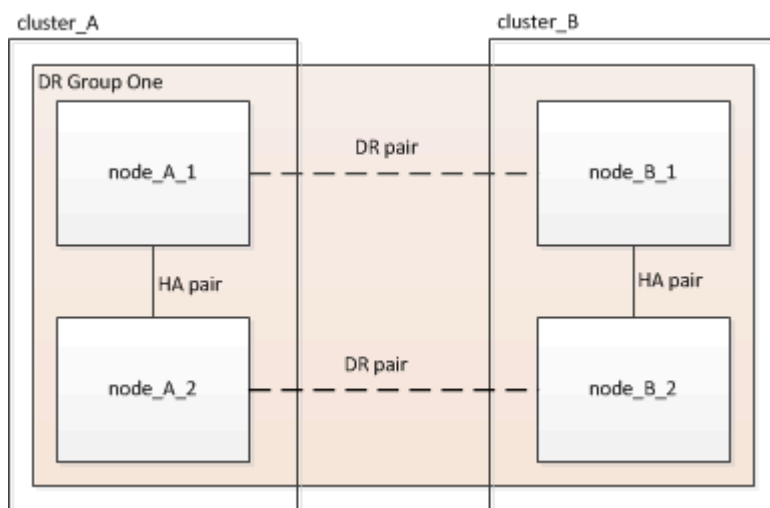
About this task

- The nodes must be running ONTAP 9 in a MetroCluster FC configuration.

This procedure is not supported on earlier versions of ONTAP or in MetroCluster IP configurations.

- The existing MetroCluster FC configuration must be healthy.
- The equipment you are adding must be supported and meet all the requirements described in [Fabric-attached MetroCluster installation and configuration](#)
- You must have available FC switch ports to accommodate the new controllers and any new bridges.
- You need the admin password and access to an FTP or SCP server.
- This procedure applies only to MetroCluster FC configurations.
- This procedure is nondisruptive and takes approximately one day to complete (excluding rack and stack) when disks are zeroed.

Before performing this procedure, the MetroCluster FC configuration consists of four nodes, with one HA pair at each site:



At the conclusion of this procedure, the MetroCluster FC configuration consists of two HA pairs at each site:



Both sites must be expanded equally. A MetroCluster FC configuration cannot consist of an uneven number of nodes.

Determining the new cabling layout

You must determine the cabling for the new controller modules and any new disk shelves to the existing FC switches.

About this task

This task must be performed at each MetroCluster site.

Steps

1. Use the procedure in [Fabric-attached MetroCluster installation and configuration](#) to create a cabling layout for your switch type, using the port usage for an eight-node MetroCluster configuration.

The FC switch port usage must match the usage described in the procedure so that the Reference Configuration Files (RCFs) can be used.



If your environment cannot be cabled in such a way that RCF files can be used, you must manually configure the system according to instructions found in [Fabric-attached MetroCluster installation and configuration](#). Do not use this procedure if the cabling cannot use RCF files.

Racking the new equipment

You must rack the equipment for the new nodes.

Steps

1. Use the procedure in [Fabric-attached MetroCluster installation and configuration](#) to rack the new storage systems, disk shelves, and FC-to-SAS bridges.

Verifying the health of the MetroCluster configuration

You should check the health of the MetroCluster configuration to verify proper operation.

Steps

1. Check that the MetroCluster is configured and in normal mode on each cluster:

```
metrocluster show
```

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

2. Check that mirroring is enabled on each node:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
        node_A_1      configured    enabled    normal
        cluster_B
        node_B_1      configured    enabled    normal
2 entries were displayed.
```

3. Check that the MetroCluster components are healthy:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
```

```
Last Checked On: 10/1/2014 16:03:37
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results. To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

4. Check that there are no health alerts:

```
system health alert show
```

5. Simulate a switchover operation:

- From any node's prompt, change to the advanced privilege level:

```
set -privilege advanced
```

You need to respond with **y** when prompted to continue into advanced mode and see the advanced mode prompt (*>).

- Perform the switchover operation with the -simulate parameter:

```
metrocluster switchover -simulate
```

- Return to the admin privilege level:

```
set -privilege admin
```

Checking for MetroCluster configuration errors with Config Advisor

You can go to the NetApp Support Site and download the Config Advisor tool to check for common configuration errors.

About this task

Config Advisor is a configuration validation and health check tool. You can deploy it at both secure sites and non-secure sites for data collection and system analysis.



Support for Config Advisor is limited, and available only online.

Steps

1. Go to the Config Advisor download page and download the tool.

[NetApp Downloads: Config Advisor](#)

2. Run Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Sending a custom AutoSupport message prior to adding nodes to the MetroCluster configuration

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.

About this task

This task must be performed on each MetroCluster site.

Steps

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

```
system node autosupport invoke -node * -type all -message MAINT=maintenance-  
window-in-hours
```

The `maintenance-window-in-hours` parameter specifies the length of the maintenance window and can be a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can issue the following command to indicating that the maintenance period has ended:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Repeat this step on the partner site.

Recable and zone a switch fabric for the new nodes

Disconnecting the existing DR group from the fabric

You must disconnect the existing controller modules from the FC switches in the fabric.

About this task

This task must be performed at each MetroCluster site.

Steps

1. Disable the HBA ports that connect the existing controller modules to the switch fabric undergoing maintenance:

```
storage port disable -node node-name -port port-number
```

2. On the local FC switches, remove the cables from the ports for the existing controller module's HBA, FC-VI, and ATTO bridges.

You should label the cables for easy identification when you re-cable them. Only the ISL ports should remain cabled.

Applying the RCF files and recabling the switches

You must apply the RCF files to reconfigure your zoning to accommodate the new nodes.

Steps

1. Locate the RCF files for your configuration.

You must use the RCF files for an eight-node configuration and that match your switch model.

2. Apply the RCF files, following the directions on the download page, adjusting the ISL settings as needed.
3. Ensure that the switch configuration is saved.
4. Reboot the FC switches.
5. Cable both the pre-existing and the new FC-to-SAS bridges to the FC switches, using the cabling layout you created previously.

The FC switch port usage must match the MetroCluster eight-node usage described in [Fabric-attached MetroCluster installation and configuration](#) so that the Reference Configuration Files (RCFs) can be used.



If your environment cannot be cabled in such a way that RCF files can be used then contact technical support. Do NOT use this procedure if the cabling cannot use RCF files.

6. Verify that the ports are online by using the correct command for your switch.

Switch vendor	Command
Brocade	switchshow
Cisco	show interface brief

7. Use the procedure in [Fabric-attached MetroCluster installation and configuration](#) to cable the FC-VI ports from the existing and new controllers, using the cabling layout you created previously.

The FC switch port usage must match the MetroCluster eight-node usage described in [Fabric-attached MetroCluster installation and configuration](#) so that the Reference Configuration Files (RCFs) can be used.



If your environment cannot be cabled in such a way that RCF files can be used then contact technical support. Do NOT use this procedure if the cabling cannot use RCF files.

8. From the existing nodes, verify that the FC-VI ports are online:

```
metrocluster interconnect adapter show
```

```
metrocluster interconnect mirror show
```

9. Cable the HBA ports from the current and the new controllers.
10. On the existing controller modules, e-enable the ports connected to the switch fabric undergoing maintenance:

```
storage port enable -node node-name -port port-ID
```

11. Start the new controllers and boot them into Maintenance mode:

```
boot_ontap maint
```

12. Verify that only storage that will be used by the new DR group is visible to the new controller modules.

None of the storage that is used by the other DR group should be visible.

13. Return to the beginning of this process to re-cable the second switch fabric.

Configure ONTAP on the new controllers

Clearing the configuration on a controller module

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

Steps

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
```

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.

Assigning disk ownership in AFF systems

If you are using AFF systems in a configuration with mirrored aggregates and the nodes do not have the disks (SSDs) correctly assigned, you should assign half the disks on each shelf to one local node and the other half of the disks to its HA partner node. You should create a configuration in which each node has the same number of disks in its

local and remote disk pools.

About this task

The storage controllers must be in Maintenance mode.

This does not apply to configurations which have unmirrored aggregates, an active/passive configuration, or that have an unequal number of disks in local and remote pools.

This task is not required if disks were correctly assigned when received from the factory.



Pool 0 always contains the disks that are found at the same site as the storage system that owns them, while Pool 1 always contains the disks that are remote to the storage system that owns them.

Steps

1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disks to the nodes located at the first site (site A):

You should assign an equal number of disks to each pool.

- a. On the first node, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:

```
disk assign -disk disk-name -p pool -n number-of-disks
```

If storage controller Controller_A_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

- b. Repeat the process for the second node at the local site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:

```
disk assign -disk disk-name -p pool
```

If storage controller Controller_A_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Assign the disks to the nodes located at the second site (site B):

You should assign an equal number of disks to each pool.

- a. On the first node at the remote site, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:

```
disk assign -disk disk-name -p pool
```

If storage controller Controller_B_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

- b. Repeat the process for the second node at the remote site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:

```
disk assign -disk disk-name -p pool
```

If storage controller Controller_B_2 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirm the disk assignments:

```
storage show disk
```

5. Exit Maintenance mode:

```
halt
```

6. Display the boot menu:

```
boot_ontap menu
```

7. On each node, select option **4** to initialize all disks.

Assigning disk ownership in non-AFF systems

If the MetroCluster nodes do not have the disks correctly assigned, or if you are using DS460C disk shelves in your configuration, you must assign disks to each of the nodes in the MetroCluster configuration on a shelf-by-shelf basis. You will create a configuration in which each node has the same number of disks in its local and remote disk pools.

About this task

The storage controllers must be in Maintenance mode.

If your configuration does not include DS460C disk shelves, this task is not required if disks were correctly assigned when received from the factory.



- Pool 0 always contains the disks that are found at the same site as the storage system that owns them.
- Pool 1 always contains the disks that are remote to the storage system that owns them.

If your configuration includes DS460C disk shelves, you should manually assign the disks using the following guidelines for each 12-disk drawer:

Assign these disks in the drawer...	To this node and pool...
0 - 2	Local node's pool 0
3 - 5	HA partner node's pool 0
6 - 8	DR partner of the local node's pool 1
9 - 11	DR partner of the HA partner's pool 1

This disk assignment pattern ensures that an aggregate is minimally affected in case a drawer goes offline.

Steps

1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disk shelves to the nodes located at the first site (site A):

Disk shelves at the same site as the node are assigned to pool 0 and disk shelves located at the partner site are assigned to pool 1.

You should assign an equal number of shelves to each pool.

- a. On the first node, systematically assign the local disk shelves to pool 0 and the remote disk shelves to pool 1:

```
disk assign -shelf local-switch-name:shelf-name.port -p pool
```

If storage controller Controller_A_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

- b. Repeat the process for the second node at the local site, systematically assigning the local disk

shelves to pool 0 and the remote disk shelves to pool 1:

```
disk assign -shelf local-switch-name:shelf-name.port -p pool
```

If storage controller Controller_A_2 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. Assign the disk shelves to the nodes located at the second site (site B):

Disk shelves at the same site as the node are assigned to pool 0 and disk shelves located at the partner site are assigned to pool 1.

You should assign an equal number of shelves to each pool.

- a. On the first node at the remote site, systematically assign its local disk shelves to pool 0 and its remote disk shelves to pool 1:

```
disk assign -shelf local-switch-namesshelf-name -p pool
```

If storage controller Controller_B_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

- b. Repeat the process for the second node at the remote site, systematically assigning its local disk shelves to pool 0 and its remote disk shelves to pool 1:

```
disk assign -shelf shelf-name -p pool
```

If storage controller Controller_B_2 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confirm the shelf assignments:

```
storage show shelf
```

5. Exit Maintenance mode:

```
halt
```

6. Display the boot menu:

```
boot_ontap menu
```

7. On each node, select option **4** to initialize all disks.

Verifying the ha-config state of components

In a MetroCluster configuration, the ha-config state of the controller module and chassis components must be set to **mcc** so they boot up properly.

About this task

- The system must be in Maintenance mode.
- This task must be performed on each new controller module.

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".

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

```
ha-config modify controller mcc
```

3. If the displayed system state of the chassis is not correct, set the HA state for the chassis:

```
ha-config modify chassis mcc
```

4. Repeat these steps on the other replacement node.

Booting the new controllers and joining them to the cluster

To join the new controllers to the cluster, you must boot each new controller module and use the ONTAP cluster setup wizard to identify the cluster will join.

Before you begin

You must have cabled the MetroCluster configuration.

You must not have configured the Service Processor prior to performing this task.

About this task

This task must be performed on each of the new controllers at both clusters in the MetroCluster configuration.

Steps

1. If you have not already done so, power up each node and let them boot completely.

If the system is in Maintenance mode, issue the `halt` command to exit Maintenance mode, and then issue the following command from the LOADER prompt:

```
boot_ontap
```

The controller module enters the node setup wizard.

The output should be similar to the following:

```
Welcome to node setup
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the setup wizard.  
                Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
.  
.   
.
```

2. Enable the AutoSupport tool by following the directions provided by the system.
3. Respond to the prompts to configure the node management interface.

The prompts are similar to the following:

```
Enter the node management interface port: [e0M]:  
Enter the node management interface IP address: 10.228.160.229  
Enter the node management interface netmask: 225.225.252.0  
Enter the node management interface default gateway: 10.228.160.1
```

4. Confirm that nodes are configured in high-availability mode:

```
storage failover show -fields mode
```

If not, you must issue the following command on each node, and then reboot the node:

```
storage failover modify -mode ha -node localhost
```

This command configures high availability mode but does not enable storage failover. Storage failover is automatically enabled when you issue the `metrocluster configure` command later in the configuration process.

5. Confirm that you have four ports configured as cluster interconnects:

```
network port show
```

The following example shows output for two controllers in cluster_A. If it is a two-node MetroCluster configuration, the output shows only one node.

```
cluster_A::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----

node_A_1						
	**e0a	Cluster	Cluster	up	1500	
	auto/1000					
	e0b	Cluster	Cluster	up	1500	
	auto/1000**					
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
node_A_2						
	**e0a	Cluster	Cluster	up	1500	
	auto/1000					
	e0b	Cluster	Cluster	up	1500	
	auto/1000**					
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
14 entries were displayed.						

6. Because you are using the CLI to set up the cluster, exit the Node Setup wizard:

```
exit
```

7. Log in to the admin account by using the admin user name.

8. Start the Cluster Setup wizard, and then join the existing cluster:

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

Do you want to create a new cluster or join an existing cluster?
{create, join}:`join`

9. After you complete the **Cluster Setup** wizard and it exits, verify that the cluster is active and the node is healthy:

```
cluster show
```

The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

```
cluster_A::> cluster show
Node                Health  Eligibility
-----
node_A_1            true   true
node_A_2            true   true
node_A_3            true   true
```

If it becomes necessary to change any of the settings you entered for the admin SVM or node SVM, you can access the **Cluster Setup** wizard by using the `cluster setup` command.

Configure the clusters into a MetroCluster configuration

Configure intercluster LIFs

Configuring intercluster LIFs on dedicated ports

You can configure intercluster LIFs on dedicated ports. Doing so typically increases the available bandwidth for replication traffic.

Steps

1. List the ports in the cluster:

network port show

For complete command syntax, see the man page.

The following example shows the network ports in cluster01:

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	

cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000

2. Determine which ports are available to dedicate to intercluster communication:

network interface show -fields home-port,curr-port

For complete command syntax, see the man page.

The following example shows that ports "e0e" and "e0f" have not been assigned LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1  e0a      e0a
Cluster cluster01-01_clus2  e0b      e0b
Cluster cluster01-02_clus1  e0a      e0a
Cluster cluster01-02_clus2  e0b      e0b
cluster01
      cluster_mgmt          e0c      e0c
cluster01
      cluster01-01_mgmt1    e0c      e0c
cluster01
      cluster01-02_mgmt1    e0c      e0c
```

3. Create a failover group for the dedicated ports:

```
network interface failover-groups create -vserver system_SVM -failover-group
failover_group -targets physical_or_logical_ports
```

The following example assigns ports "e0e" and "e0f" to the failover group "intercluster01" on the system SVM "cluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

```
network interface failover-groups show
```

For complete command syntax, see the man page.

```

cluster01::> network interface failover-groups show

```

Vserver	Group	Failover Targets
Cluster	Cluster	cluster01-01:e0a, cluster01-01:e0b, cluster01-02:e0a, cluster01-02:e0b
cluster01	Default	cluster01-01:e0c, cluster01-01:e0d, cluster01-02:e0c, cluster01-02:e0d, cluster01-01:e0e, cluster01-01:e0f cluster01-02:e0e, cluster01-02:e0f
	intercluster01	cluster01-01:e0e, cluster01-01:e0f cluster01-02:e0e, cluster01-02:e0f

5. Create intercluster LIFs on the system SVM and assign them to the failover group.

ONTAP version	Command
9.6 and later	network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group
9.5 and earlier	network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group

For complete command syntax, see the man page.

The following example creates intercluster LIFs "cluster01_icl01" and "cluster01_icl02" in the failover group "intercluster01":


```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01

```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster
```

For complete command syntax, see the man page.

```

cluster01::> network interface show -service-policy default-intercluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0e
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0f
true				

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster -failover
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster -failover
```

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs "cluster01_icl01" and "cluster01_icl02" on the SVM "e0e" port will fail over to the "e0f" port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01			Failover Targets: cluster01-01:e0e, cluster01-01:e0f	
cluster01	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01			Failover Targets: cluster01-02:e0e, cluster01-02:e0f	

Configuring intercluster LIFs on shared data ports

You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

Steps

1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

The following example shows the network ports in cluster01:

```
cluster01::> network port show
```

(Mbps)						Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000

2. Create intercluster LIFs on the system SVM:

In ONTAP 9.6 and later:

```
network interface create -vserver system_SVM -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

In ONTAP 9.5 and earlier:

```
network interface create -vserver system_SVM -lif LIF_name -role intercluster
-home-node node -home-port port -address port_IP -netmask netmask
```

For complete command syntax, see the man page.

The following example creates intercluster LIFs cluster01_icl01 and cluster01_icl02:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster
```

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-intercluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01	e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02	e0c
true					

4. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster -failover
```

In ONTAP 9.5 and earlier:

```
network interface show -role intercluster -failover
```

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs "cluster01_icl01" and "cluster01_icl02" on the "e0c" port will fail over to the "e0d" port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-01:e0c, cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-02:e0c, cluster01-02:e0d	

Mirroring the root aggregates

You must mirror the root aggregates to provide data protection.

By default, the root aggregate is created as RAID-DP type aggregate. You can change the root aggregate from RAID-DP to RAID4 type aggregate. The following command modifies the root aggregate for RAID4 type aggregate:

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```



On non-ADP systems, the RAID type of the aggregate can be modified from the default RAID-DP to RAID4 before or after the aggregate is mirrored.

Steps

1. Mirror the root aggregate:

```
storage aggregate mirror aggr_name
```

The following command mirrors the root aggregate for controller_A_1:

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

This mirrors the aggregate, so it consists of a local plex and a remote plex located at the remote MetroCluster site.

2. Repeat the previous step for each node in the MetroCluster configuration.

Implementing the MetroCluster configuration

You must run the `metrocluster configure -refresh true` command to start data

protection on the nodes that you have added to a MetroCluster configuration.

About this task

You issue the `metrocluster configure -refresh true` command once, on one of the newly added nodes, to refresh the MetroCluster configuration. You do not need to issue the command on each of the sites or nodes.

The `metrocluster configure -refresh true` command automatically pairs the two nodes with the lowest system IDs in each of the two clusters as disaster recovery (DR) partners. In a four-node MetroCluster configuration, there are two DR partner pairs. The second DR pair is created from the two nodes with higher system IDs.

Steps

1. Refresh the MetroCluster configuration:

- a. Enter advanced privilege mode:

```
set -privilege advanced
```

- b. Refresh the MetroCluster configuration on one of the new nodes:

```
metrocluster configure -refresh true
```

The following example shows the MetroCluster configuration refreshed on both DR groups:

```
controller_A_2::*> metrocluster configure -refresh true  
  
[Job 726] Job succeeded: Configure is successful.
```

```
controller_A_4::*> metrocluster configure -refresh true  
  
[Job 740] Job succeeded: Configure is successful.
```

- c. Return to admin privilege mode:

```
set -privilege admin
```

2. Verify the networking status on site A:

```
network port show
```

The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper
controller_A_1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
controller_A_2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

```
14 entries were displayed.
```

3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration:

a. Verify the configuration from site A:

```
metrocluster show
```

```
cluster_A::> metrocluster show
```

```
Configuration: IP fabric
```

Cluster	Entry Name	State
Local: cluster_A	Configuration state	configured
	Mode	normal
Remote: cluster_B	Configuration state	configured
	Mode	normal

b. Verify the configuration from site B:

```
metrocluster show
```

```
cluster_B::> metrocluster show
```

```
Configuration: IP fabric
```

Cluster	Entry Name	State
-----	-----	-----
Local: cluster_B	Configuration state	configured
	Mode	normal
Remote: cluster_A	Configuration state	configured
	Mode	normal

Creating a mirrored data aggregate on each node

You must create a mirrored data aggregate on each node in the DR group.

About this task

- You should know what drives will be used in the new aggregate.
- If you have multiple drive types in your system (heterogeneous storage), you should understand how you can ensure that the correct drive type is selected.
- Drives are owned by a specific node; when you create an aggregate, all drives in that aggregate must be owned by the same node, which becomes the home node for that aggregate.

In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions.

- Aggregate names should conform to the naming scheme you determined when you planned your MetroCluster configuration.

Disk and aggregate management

Steps

1. Display a list of available spares:

```
storage disk show -spare -owner node_name
```

2. Create the aggregate:

```
storage aggregate create -mirror true
```

If you are logged in to the cluster on the cluster management interface, you can create an aggregate on any node in the cluster. To ensure that the aggregate is created on a specific node, use the `-node` parameter or specify drives that are owned by that node.

You can specify the following options:

- Aggregate's home node (that is, the node that owns the aggregate in normal operation)
- List of specific drives that are to be added to the aggregate
- Number of drives to include



In the minimum supported configuration, in which a limited number of drives are available, you must use the `force-small-aggregate` option to allow the creation of a three disk RAID-DP aggregate.

- Checksum style to use for the aggregate
- Type of drives to use
- Size of drives to use
- Drive speed to use
- RAID type for RAID groups on the aggregate
- Maximum number of drives that can be included in a RAID group
- Whether drives with different RPM are allowed

For more information about these options, see the `storage aggregate create` man page.

The following command creates a mirrored aggregate with 10 disks:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10
-node node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verify the RAID group and drives of your new aggregate:

```
storage aggregate show-status -aggregate aggregate-name
```

Configuring FC-to-SAS bridges for health monitoring

About this task

- Third-party SNMP monitoring tools are not supported for FibreBridge bridges.
- Beginning with ONTAP 9.8, FC-to-SAS bridges are monitored via in-band connections by default, and additional configuration is not required.



Beginning with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

Step

1. From the ONTAP cluster prompt, add the bridge to health monitoring:
 - a. Add the bridge, using the command for your version of ONTAP:

ONTAP version	Command
9.5 and later	<code>storage bridge add -address 0.0.0.0 -managed-by in-band -name <i>bridge-name</i></code>

```
storage bridge add -address bridge-  
ip-address -name bridge-name
```

- b. Verify that the bridge has been added and is properly configured:

```
storage bridge show
```

It might take as long as 15 minutes to reflect all data because of the polling interval. The ONTAP health monitor can contact and monitor the bridge if the value in the "Status" column is "ok", and other information, such as the worldwide name (WWN), is displayed.

The following example shows that the FC-to-SAS bridges are configured:

```
controller_A_1::> storage bridge show
```

Bridge	Symbolic Name	Is Monitored	Monitor Status
Vendor Model	Bridge WWN		
ATTO_10.10.20.10	atto01	true	ok
FibreBridge 7500N	20000010867038c0		
ATTO_10.10.20.11	atto02	true	ok
FibreBridge 7500N	20000010867033c0		
ATTO_10.10.20.12	atto03	true	ok
FibreBridge 7500N	20000010867030c0		
ATTO_10.10.20.13	atto04	true	ok
FibreBridge 7500N	2000001086703b80		

```
4 entries were displayed
```

```
controller_A_1::>
```

Moving a metadata volume in MetroCluster configurations

You can move a metadata volume from one aggregate to another aggregate in a MetroCluster configuration. You might want to move a metadata volume when the source aggregate is decommissioned or unmirrored, or for other reasons that make the aggregate ineligible.

About this task

- You must have cluster administrator privileges to perform this task.
- The target aggregate must be mirrored and should not be in the degraded state.
- The available space in the target aggregate must be larger than the metadata volume that you are moving.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Identify the metadata volume that should be moved:

```
volume show MDV_CRS*
```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume                Aggregate      State      Type      Size
Available Used%
-----
Cluster_A
MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
Node_A_1_aggr1
online     RW        10GB
9.50GB    5%
Cluster_A
MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
Node_A_2_aggr1
online     RW        10GB
9.50GB    5%
Cluster_A
MDV_CRS_15035e66c9f311e7902700a098439625_A
Node_B_1_aggr1
-          RW        -
-          -
Cluster_A
MDV_CRS_15035e66c9f311e7902700a098439625_B
Node_B_2_aggr1
-          RW        -
-          -
4 entries were displayed.

Cluster_A::>
```

3. Identify an eligible target aggregate:

```
metrocluster check config-replication show-aggregate-eligibility
```

The following command identifies the aggregates in cluster_A that are eligible to host metadata volumes:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-eligibility
```

```
Aggregate Hosted Config Replication Vols Host Addl Vols Comments
-----
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```



In the previous example, Node_A_1_aggr2 and Node_A_2_aggr2 are eligible.

4. Start the volume move operation:

```
volume move start -vserver svm_name -volume metadata_volume_name -destination
-aggregate destination_aggregate_name*
```

The following command moves metadata volume "MDV_CRS_14c00d4ac9f311e7922800a0984395f1" from "aggregate Node_A_1_aggr1" to "aggregate Node_A_1_aggr2":

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
        "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A". This may cause
severe
        performance or stability problems. Do not proceed unless
directed to
        do so by support. Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verify the state of the volume move operation:

```
volume move show -volume vol_constituent_name
```

6. Return to the admin privilege level:

```
set -privilege admin
```

Checking the MetroCluster configuration

You can check that the components and relationships in the MetroCluster configuration are working correctly. You should do a check after initial configuration and after making any changes to the MetroCluster configuration. You should also do a check before a negotiated (planned) switchover or a switchback operation.

About this task

If the `metrocluster check run` command is issued twice within a short time on either or both clusters, a conflict can occur and the command might not collect all data. Subsequent `metrocluster check show` commands do not show the expected output.

Steps

1. Check the configuration:

```
metrocluster check run
```

The command runs as a background job and might not be completed immediately.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show
Last Checked On: 9/13/2018 20:41:37
```

Component	Result
-----	-----
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	ok
6 entries were displayed.	

2. Display more detailed results from the most recent `metrocluster check run` command:

```
metrocluster check aggregate show
```

```
metrocluster check cluster show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

The `metrocluster check show` commands show the results of the most recent `metrocluster check run` command. You should always run the `metrocluster check run` command prior to using the `metrocluster check show` commands so that the information displayed is current.

The following example shows the `metrocluster check aggregate show` command output for a healthy four-node MetroCluster configuration:

```
cluster_A::> metrocluster check aggregate show
```

```
Last Checked On: 8/5/2014 00:42:58
```

Node Result	Aggregate	Check
-----	-----	-----
controller_A_1	controller_A_1_aggr0	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok	controller_A_1_aggr1	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok	controller_A_1_aggr2	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok		

```

controller_A_2      controller_A_2_aggr0
ok
                        mirroring-status
                        disk-pool-allocation
ok
                        ownership-state
ok
                        controller_A_2_aggr1
                        mirroring-status
ok
                        disk-pool-allocation
ok
                        ownership-state
ok
                        controller_A_2_aggr2
                        mirroring-status
ok
                        disk-pool-allocation
ok
                        ownership-state
ok

18 entries were displayed.

```

The following example shows the `metrocluster check cluster show` command output for a healthy four-node MetroCluster configuration. It indicates that the clusters are ready to perform a negotiated switchover if necessary.

Last Checked On: 9/13/2017 20:47:04

Cluster	Check	Result
mccint-fas9000-0102	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok
mccint-fas9000-0304	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok

10 entries were displayed.

Checking for MetroCluster configuration errors with Config Advisor

You can go to the NetApp Support Site and download the Config Advisor tool to check for common configuration errors.

About this task

Config Advisor is a configuration validation and health check tool. You can deploy it at both secure sites and non-secure sites for data collection and system analysis.



Support for Config Advisor is limited, and available only online.

Steps

1. Go to the Config Advisor download page and download the tool.

[NetApp Downloads: Config Advisor](#)

2. Run Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Sending a custom AutoSupport message after to adding nodes to the MetroCluster configuration

You should issue an AutoSupport message to notify NetApp technical support that maintenance is complete.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.
2. Invoke an AutoSupport message indicating the end of the maintenance:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Repeat this step on the partner site.

Verifying switchover, healing, and switchback

You should verify the switchover, healing, and switchback operations of the MetroCluster configuration.

Steps

1. Use the procedures for negotiated switchover, healing, and switchback in [MetroCluster management and disaster recovery](#).

Expanding a four-node MetroCluster IP configuration to an eight-node configuration

Beginning with ONTAP 9.9.1, you can add four new nodes to the MetroCluster IP configuration as a second DR group. This creates an eight-node MetroCluster configuration.

Before you begin

- The old and new nodes must be running the same version of ONTAP.
- You must ensure that the old and new platform models are supported for platform mixing.

[NetApp Hardware Universe](#)

- You must ensure that the old and new platform models are both supported by the IP switches.

[NetApp Hardware Universe](#)

- The new nodes must have enough storage to accommodate the data of the old nodes, along with adequate disks for root aggregates and spare disks.

Example naming in this procedure

This procedure uses example names throughout to identify the DR groups, nodes, and switches involved.

DR groups	cluster_A at site_A	cluster_B at site_B
dr_group_1-old	<ul style="list-style-type: none">• node_A_1-old• node_A_2-old	<ul style="list-style-type: none">• node_B_1-old• node_B_2-old
dr_group_2-new	<ul style="list-style-type: none">• node_A_3-new• node_A_4-new	<ul style="list-style-type: none">• node_B_3-new• node_B_4-new

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.

About this task

This task must be performed on each MetroCluster site.

Steps

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

- a. Issue the following command:

```
system node autosupport invoke -node * -type all -message "MAINT=10h  
Upgrading old-model to new-model"
```

This example specifies a 10 hour maintenance window. You might want to allow additional time, depending on your plan.

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.

Verifying the health of the MetroCluster configuration

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

Steps

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

- a. Check whether the system is multipathed:

```
node run -node node-name sysconfig -a
```

- b. Check for any health alerts on both clusters:

```
system health alert show
```

- c. Confirm the MetroCluster configuration and that the operational mode is normal:

```
metrocluster show
```

- d. Perform a MetroCluster check:

```
metrocluster check run
```

- e. Display the results of the MetroCluster check:

```
metrocluster check show
```

f. Run Config Advisor.

[NetApp Downloads: Config Advisor](#)

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

2. Verify that the cluster is healthy:

```
cluster show -vserver Cluster
```

```
cluster_A::> cluster show -vserver Cluster
Node           Health  Eligibility  Epsilon
-----
node_A_1       true    true         false
node_A_2       true    true         false

cluster_A::>
```

3. Verify that all cluster ports are up:

```
network port show -ipspace cluster
```

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

Port          IPspace      Broadcast Domain Link MTU  Speed(Mbps) Health
-----
e0a           Cluster      Cluster      up   9000  auto/10000 healthy
e0b           Cluster      Cluster      up   9000  auto/10000 healthy

Node: node_A_2-old

Port          IPspace      Broadcast Domain Link MTU  Speed(Mbps) Health
-----
e0a           Cluster      Cluster      up   9000  auto/10000 healthy
e0b           Cluster      Cluster      up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verify that all cluster LIFs are up and operational:

```
network interface show -vserver Cluster
```

Each cluster LIF should display true for Is Home and have a Status Admin/Oper of up/up

```
cluster_A::> network interface show -vserver cluster
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	-----				
Cluster					
	node_A_1-old_clus1	up/up	169.254.209.69/16	node_A_1	e0a
true					
	node_A_1-old_clus2	up/up	169.254.49.125/16	node_A_1	e0b
true					
	node_A_2-old_clus1	up/up	169.254.47.194/16	node_A_2	e0a
true					
	node_A_2-old_clus2	up/up	169.254.19.183/16	node_A_2	e0b
true					

```
4 entries were displayed.
```

```
cluster_A::>
```

5. Verify that auto-revert is enabled on all cluster LIFs:

```
network interface show -vserver Cluster -fields auto-revert
```

```

cluster_A::> network interface show -vserver Cluster -fields auto-revert

      Logical
Vserver  Interface      Auto-revert
-----  -
Cluster
      node_A_1-old_clus1
                        true
      node_A_1-old_clus2
                        true
      node_A_2-old_clus1
                        true
      node_A_2-old_clus2
                        true

      4 entries were displayed.

cluster_A::>

```

Removing the configuration from monitoring applications

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

Steps

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

If you are using...	Use this procedure...
Tiebreaker	Removing MetroCluster Configurations.
Mediator	Issue the following command from the ONTAP prompt: <pre>metrocluster configuration-settings mediator remove</pre>
Third-party applications	Refer to the product documentation.

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

Preparing the new controller modules

You must prepare the four new MetroCluster nodes and install the correct ONTAP version.

About this task

This task must be performed on each of the new nodes:

- node_A_3-new
- node_A_4-new
- node_B_3-new
- node_B_4-new

In these steps, you clear the configuration on the nodes and clear the mailbox region on new drives.

Steps

1. Rack the new controllers.
2. Cable the new MetroCluster IP nodes to the IP switches as shown in the *MetroCluster installation and configuration*.

Cabling the IP switches

3. Configure the MetroCluster IP nodes using the following sections of the *MetroCluster installation and configuration*.
 - a. [Gathering required information](#)
 - b. [Restoring system defaults on a controller module](#)
 - c. [Verifying the ha-config state of components](#)
 - d. [Manually assigning drives for pool 0 \(ONTAP 9.4 and later\)](#)
4. From Maintenance mode, issue the halt command to exit Maintenance mode, and then issue the boot_ontap command to boot the system and get to cluster setup.

Do not complete the cluster wizard or node wizard at this time.

Joining the new nodes to the clusters

You must add the four new MetroCluster IP nodes to the existing MetroCluster configuration.

About this task

You must perform this task on both clusters.

Steps

1. Add the new MetroCluster IP nodes to the existing MetroCluster configuration.
 - a. Join the first new MetroCluster IP node (node_A_1-new) to the existing MetroCluster IP configuration.

```
Welcome to the cluster setup wizard.
```

```
You can enter the following commands at any time:
```

"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".

To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp Technical

Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and

resolution, should a problem occur on your system.

For further information on AutoSupport, see:

<http://support.netapp.com/autosupport/>

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: 172.17.8.93

172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.

Examples of

node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.

Enter the node management interface port [e0M]:

Enter the node management interface IP address: 172.17.8.93

Enter the node management interface netmask: 255.255.254.0

Enter the node management interface default gateway: 172.17.8.1

A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
<https://172.17.8.93>

Otherwise, press Enter to complete cluster setup using the command
line
interface:

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

```
Existing cluster interface configuration found:
```

Port	MTU	IP	Netmask
e0c	9000	169.254.148.217	255.255.0.0
e0d	9000	169.254.144.238	255.255.0.0

```
Do you want to use this configuration? {yes, no} [yes]: yes
```

```
.
.
.
```

b. Join the second new MetroCluster IP node (node_A_2-new) to the existing MetroCluster IP configuration.

2. Repeat these steps to join node_B_1-new and node_B_2-new to cluster_B.

Configuring intercluster LIFs, creating the MetroCluster interfaces, and mirroring root aggregates

You must create cluster peering LIFs, create the MetroCluster interfaces on the new MetroCluster IP nodes.

About this task

The home port used in the examples are platform-specific. You should use the appropriate home port specific to MetroCluster IP node platform.

Steps

1. On the new MetroCluster IP nodes, configure the intercluster LIFs using the following procedures:

[Configuring intercluster LIFs on dedicated ports](#)

[Configuring intercluster LIFs on shared data ports](#)

2. On each site, verify that cluster peering is configured:

```
cluster peer show
```

The following example shows the cluster peering configuration on cluster_A:


```
cluster_A:> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
cluster_B              1-80-000011      Available      ok
```

The following example shows the cluster peering configuration on cluster_B:

```
cluster_B:> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
cluster_A              1-80-000011      Available      ok
cluster_B::>
```

3. Create the DR group for the MetroCluster IP nodes:

```
metrocluster configuration-settings dr-group create -partner-cluster
```

For more information on the MetroCluster configuration settings and connections, see the following:

[Considerations for MetroCluster IP configurations](#)

[Creating the DR group](#)

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Verify that the DR group was created.

```
metrocluster configuration-settings dr-group show
```

```
cluster_A::> metrocluster configuration-settings dr-group show
```

DR Group ID	Cluster	Node	DR Partner
1	cluster_A	node_A_1-old	node_B_1-old
		node_A_2-old	node_B_2-old
	cluster_B	node_B_1-old	node_A_1-old
		node_B_2-old	node_A_2-old
2	cluster_A	node_A_1-new	node_B_1-new
		node_A_2-new	node_B_2-new
	cluster_B	node_B_1-new	node_A_1-new
		node_B_2-new	node_A_2-new

8 entries were displayed.

```
cluster_A::>
```

5. Configure the MetroCluster IP interfaces for the newly joined MetroCluster IP nodes:

```
metrocluster configuration-settings interface create -cluster-name
```



- Certain platforms use a VLAN for the MetroCluster IP interface. By default, each of the two ports use a different VLAN: 10 and 20. You can also specify a different (non-default) VLAN higher than 100 (between 101 and 4095) using the `-vlan-id` parameter in the `metrocluster configuration-settings interface create` command.
- Beginning with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to [Considerations for layer 3 wide-area networks](#).

The following platform models use VLANs and allow configuration of a non-default VLAN ID.

AFF platforms	FAS platforms
<ul style="list-style-type: none"> • AFF A220 • AFF A250 • AFF A400 	<ul style="list-style-type: none"> • FAS2750 • FAS500f • FAS8300 • FAS8700



You can configure the MetroCluster IP interfaces from either cluster. Also, beginning with ONTAP 9.1.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter to create MetroCluster IP interfaces. Refer to [Considerations for layer 3 wide-area networks](#).

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port elb -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port elb -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port elb -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.
```

```
cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port elb -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port elb -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port elb -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port elb -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port elb -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verify the MetroCluster IP interfaces are created:

metrocluster configuration-settings interface show

```
cluster_A::>metrocluster configuration-settings interface show
```

DR

Config

Group	Cluster	Node	Network Address	Netmask	Gateway
State					

1	cluster_A	node_A_1-old	Home Port: e1a	172.17.26.10	255.255.255.0	-			
completed			Home Port: e1b	172.17.27.10	255.255.255.0	-			
completed			node_A_2-old	Home Port: e1a	172.17.26.11	255.255.255.0			
completed			Home Port: e1b	172.17.27.11	255.255.255.0	-			
completed			cluster_B	node_B_1-old	Home Port: e1a	172.17.26.13	255.255.255.0		
completed			Home Port: e1b	172.17.27.13	255.255.255.0	-			
completed			node_B_1-old	Home Port: e1a	172.17.26.12	255.255.255.0			
completed			Home Port: e1b	172.17.27.12	255.255.255.0	-			
completed			2	cluster_A	node_A_3-new	Home Port: e1a	172.17.28.10	255.255.255.0	-

```

completed
      Home Port: elb
      172.17.29.10      255.255.255.0      -
completed
      node_A_3-new
      Home Port: ela
      172.17.28.11      255.255.255.0      -
completed
      Home Port: elb
      172.17.29.11      255.255.255.0      -
completed
      cluster_B
      node_B_3-new
      Home Port: ela
      172.17.28.13      255.255.255.0      -
completed
      Home Port: elb
      172.17.29.13      255.255.255.0      -
completed
      node_B_3-new
      Home Port: ela
      172.17.28.12      255.255.255.0      -
completed
      Home Port: elb
      172.17.29.12      255.255.255.0      -
completed
8 entries were displayed.

cluster_A>

```

7. Connect the MetroCluster IP interfaces:

```
metrocluster configuration-settings connection connect
```



This command might take several minutes to complete.

```

cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>

```

8. Verify the connections are properly established: metrocluster configuration-settings connection show

```
cluster_A::> metrocluster configuration-settings connection show
```

DR	Source	Destination
Group Cluster Node	Network Address	Network Address Partner Type
Config State		
1	cluster_A	
	node_A_1-old	
	Home Port: ela	
completed	172.17.28.10	172.17.28.11 HA Partner
	Home Port: ela	
completed	172.17.28.10	172.17.28.12 DR Partner
	Home Port: ela	
completed	172.17.28.10	172.17.28.13 DR Auxiliary
	Home Port: elb	
completed	172.17.29.10	172.17.29.11 HA Partner
	Home Port: elb	
completed	172.17.29.10	172.17.29.12 DR Partner
	Home Port: elb	
completed	172.17.29.10	172.17.29.13 DR Auxiliary
	node_A_2-old	
	Home Port: ela	
completed	172.17.28.11	172.17.28.10 HA Partner
	Home Port: ela	
completed	172.17.28.11	172.17.28.13 DR Partner
	Home Port: ela	
completed	172.17.28.11	172.17.28.12 DR Auxiliary
	Home Port: elb	
completed	172.17.29.11	172.17.29.10 HA Partner
	Home Port: elb	
completed	172.17.29.11	172.17.29.13 DR Partner
	Home Port: elb	
completed	172.17.29.11	172.17.29.12 DR Auxiliary
DR	Source	Destination

Group	Cluster	Node	Network Address	Network Address	Partner	Type
Config	State					
1	cluster_B					
		node_B_2-old				
		Home Port: ela				
		172.17.28.13	172.17.28.12	HA Partner		
completed						
		Home Port: ela				
		172.17.28.13	172.17.28.11	DR Partner		
completed						
		Home Port: ela				
		172.17.28.13	172.17.28.10	DR Auxiliary		
completed						
		Home Port: elb				
		172.17.29.13	172.17.29.12	HA Partner		
completed						
		Home Port: elb				
		172.17.29.13	172.17.29.11	DR Partner		
completed						
		Home Port: elb				
		172.17.29.13	172.17.29.10	DR Auxiliary		
completed						
		node_B_1-old				
		Home Port: ela				
		172.17.28.12	172.17.28.13	HA Partner		
completed						
		Home Port: ela				
		172.17.28.12	172.17.28.10	DR Partner		
completed						
		Home Port: ela				
		172.17.28.12	172.17.28.11	DR Auxiliary		
completed						
		Home Port: elb				
		172.17.29.12	172.17.29.13	HA Partner		
completed						
		Home Port: elb				
		172.17.29.12	172.17.29.10	DR Partner		
completed						
		Home Port: elb				
		172.17.29.12	172.17.29.11	DR Auxiliary		
completed						
DR			Source	Destination		
Group	Cluster	Node	Network Address	Network Address	Partner	Type

```

Config State
-----
-----
2      cluster_A
      node_A_1-new**
      Home Port: ela
      172.17.26.10      172.17.26.11      HA Partner
completed
      Home Port: ela
      172.17.26.10      172.17.26.12      DR Partner
completed
      Home Port: ela
      172.17.26.10      172.17.26.13      DR Auxiliary
completed
      Home Port: elb
      172.17.27.10      172.17.27.11      HA Partner
completed
      Home Port: elb
      172.17.27.10      172.17.27.12      DR Partner
completed
      Home Port: elb
      172.17.27.10      172.17.27.13      DR Auxiliary
completed
      node_A_2-new
      Home Port: ela
      172.17.26.11      172.17.26.10      HA Partner
completed
      Home Port: ela
      172.17.26.11      172.17.26.13      DR Partner
completed
      Home Port: ela
      172.17.26.11      172.17.26.12      DR Auxiliary
completed
      Home Port: elb
      172.17.27.11      172.17.27.10      HA Partner
completed
      Home Port: elb
      172.17.27.11      172.17.27.13      DR Partner
completed
      Home Port: elb
      172.17.27.11      172.17.27.12      DR Auxiliary
completed

DR      Source      Destination
Group Cluster Node      Network Address Network Address Partner Type
Config State

```



```

-----
2      cluster_B
        node_B_2-new
          Home Port: ela
            172.17.26.13      172.17.26.12      HA Partner
completed
          Home Port: ela
            172.17.26.13      172.17.26.11      DR Partner
completed
          Home Port: ela
            172.17.26.13      172.17.26.10      DR Auxiliary
completed
          Home Port: elb
            172.17.27.13      172.17.27.12      HA Partner
completed
          Home Port: elb
            172.17.27.13      172.17.27.11      DR Partner
completed
          Home Port: elb
            172.17.27.13      172.17.27.10      DR Auxiliary
completed
        node_B_1-new
          Home Port: ela
            172.17.26.12      172.17.26.13      HA Partner
completed
          Home Port: ela
            172.17.26.12      172.17.26.10      DR Partner
completed
          Home Port: ela
            172.17.26.12      172.17.26.11      DR Auxiliary
completed
          Home Port: elb
            172.17.27.12      172.17.27.13      HA Partner
completed
          Home Port: elb
            172.17.27.12      172.17.27.10      DR Partner
completed
          Home Port: elb
            172.17.27.12      172.17.27.11      DR Auxiliary
completed
48 entries were displayed.

cluster_A::>

```

9. Verify disk auto-assignment and partitioning:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
```

Disk Owner	Usable Size	Shelf	Bay	Disk Type	Container Type	Container Name
1.10.4 node_B_2	-	10	4	SAS	remote	-
1.10.13 node_B_2	-	10	13	SAS	remote	-
1.10.14 node_B_1	-	10	14	SAS	remote	-
1.10.15 node_B_1	-	10	15	SAS	remote	-
1.10.16 node_B_1	-	10	16	SAS	remote	-
1.10.18 node_B_2	-	10	18	SAS	remote	-
...						
2.20.0 node_a_1	546.9GB	20	0	SAS	aggregate	aggr0_rha1_a1
2.20.3 node_a_2	546.9GB	20	3	SAS	aggregate	aggr0_rha1_a2
2.20.5 node_a_1	546.9GB	20	5	SAS	aggregate	rha1_a1_aggr1
2.20.6 node_a_1	546.9GB	20	6	SAS	aggregate	rha1_a1_aggr1
2.20.7 node_a_2	546.9GB	20	7	SAS	aggregate	rha1_a2_aggr1
2.20.10 node_a_1	546.9GB	20	10	SAS	aggregate	rha1_a1_aggr1
...						

43 entries were displayed.

```
cluster_A::>
```

10. Mirror the root aggregates:

```
storage aggregate mirror -aggregate aggr0_node_A_1-new
```



You must complete this step on each MetroCluster IP node.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
    in the following manner:

    Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)

Physical                                     Usable
Size      Position   Disk                               Type      Size
-----
-----
-          dparity    4.20.0                           SAS        -
-          parity     4.20.3                           SAS        -
-          data       4.20.1                           SAS      546.9GB
558.9GB

Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verify that the root aggregates are mirrored:

```
storage aggregate show
```

```
cluster_A::> aggr show

Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
aggr0_node_A_1-old
      349.0GB   16.84GB   95% online      1 node_A_1-old
raid_dp,
mirrored,
normal
```

```

aggr0_node_A_2-old
      349.0GB    16.84GB    95% online      1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
      467.6GB    22.63GB    95% online      1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
      467.6GB    22.62GB    95% online      1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
      1.02TB     1.01TB     1% online      1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
      1.02TB     1.01TB     1% online      1 node_A_2-old
raid_dp,

mirrored,

```

Finalizing the addition of the new nodes

You must incorporate the new DR group into the MetroCluster configuration and create mirrored data aggregates on the new nodes.

Steps

1. Create mirrored data aggregates on each of the new MetroCluster nodes:

```

storage aggregate create -aggregate aggregate-name -node node-name -diskcount
no-of-disks -mirror true

```



You must create at least one mirrored data aggregate per site. It is recommended to have two mirrored data aggregates per site on MetroCluster IP nodes to host the MDV volumes, however a single aggregate per site is supported (but not recommended). It is support that one site of the MetroCluster has a single mirrored data aggregate and the other site has more than one mirrored data aggregate.

The following example shows the creation of an aggregate on node_A_1-new.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-  
new -diskcount 10 -mirror t
```

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would be:

First Plex

RAID Group rg0, 5 disks (block checksum, raid_dp)

				Usable
Physical	Position	Disk	Type	Size
Size				
-----	-----	-----	-----	-----
-----	dparity	5.10.15	SAS	-
-	parity	5.10.16	SAS	-
-	data	5.10.17	SAS	546.9GB
547.1GB	data	5.10.18	SAS	546.9GB
558.9GB	data	5.10.19	SAS	546.9GB
558.9GB				

Second Plex

RAID Group rg0, 5 disks (block checksum, raid_dp)

				Usable
Physical	Position	Disk	Type	Size
Size				
-----	-----	-----	-----	-----
-----	dparity	4.20.17	SAS	-
-	parity	4.20.14	SAS	-

```

-
      data      4.20.18      SAS      546.9GB
547.1GB
      data      4.20.19      SAS      546.9GB
547.1GB
      data      4.20.16      SAS      546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>

```

2. Refresh the MetroCluster configuration:

a. Enter advanced privilege mode:

```
set -privilege advanced
```

b. Refresh the MetroCluster configuration on one of the new nodes:

```
metrocluster configure
```

The following example shows the MetroCluster configuration refreshed on both DR groups:

```

cluster_A::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.

```

c. Return to admin privilege mode:

```
set -privilege admin
```

3. Verify that the nodes are added to their DR group.

```
cluster_A::*> metrocluster node show
```

DR	Configuration	DR
Group Cluster Node	State	Mirroring Mode

1	cluster_A	
	node_A_1-old	configured enabled normal
	node_A_2-old	configured enabled normal
	cluster_B	
	node_B_1-old	configured enabled normal
	node_B_2-old	configured enabled normal
2	cluster_A	
	node_A_3-new	configured enabled normal
	node_A_4-new	configured enabled normal
	cluster_B	
	node_B_3-new	configured enabled normal
	node_B_4-new	configured enabled normal

8 entries were displayed.

```
cluster_A::*>
```

4. Move the MDV_CRS volumes from the old nodes to the new nodes in advanced privilege.

a. Display the volumes to identify the MDV volumes:



If you have a single mirrored data aggregate per site then move both the MDV volumes to this single aggregate. If you have two or more mirrored data aggregates, then move each MDV volume to a different aggregate.

The following example shows the MDV volumes in the `volume show` output:

```

cluster_A::> volume show
Vserver   Volume                               Aggregate   State   Type   Size
Available Used%
-----
...

cluster_A  MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
          aggr_b1             -         RW         -
-      -
cluster_A  MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
          aggr_b2             -         RW         -
-      -
cluster_A  MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
          aggr_a1      online      RW         10GB
9.50GB    0%
cluster_A  MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
          aggr_a2      online      RW         10GB
9.50GB    0%
...
11 entries were displayed.mple

```

b. Set the advanced privilege level:

```
set -privilege advanced
```

c. Move the MDV volumes, one at a time:

```

volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node
-vserver vserver-name

```

The following example shows the command and output for moving "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" to aggregate "data_a3" on "node_A_3".


```
cluster_A::> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
        "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
        performance or stability problems. Do not proceed unless
directed to
        do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

- d. Use the volume show command to check that the MDV volume has been successfully moved:

```
volume show mdv-name
```

The following output shows that the MDV volume has been successfully moved.

```
cluster_A::> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver      Volume      Aggregate      State      Type      Size
Available Used%
-----
-----
cluster_A    MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
              aggr_a2      online      RW          10GB
9.50GB      0%
```

- e. Return to admin mode:

```
set -privilege admin
```

5. Move epsilon from an old node to a new node:

- a. Identify which node currently has epsilon:

```
cluster show -fields epsilon
```

```
cluster_B::> cluster show -fields epsilon
node                epsilon
-----
node_A_1-old        true
node_A_2-old        false
node_A_3-new        false
node_A_4-new        false
4 entries were displayed.
```

- b. Set epsilon to false on the old node (node_A_1-old):

```
cluster modify -node old-node -epsilon false*
```

- c. Set epsilon to true on the new node (node_A_3-new):

```
cluster modify -node new-node -epsilon true
```

- d. Verify that epsilon has moved to the correct node:

```
cluster show -fields epsilon
```

```
cluster_A::> cluster show -fields epsilon
node                epsilon
-----
node_A_1-old        false
node_A_2-old        false
node_A_3-new        true
node_A_4-new        false
4 entries were displayed.
```

Removing a Disaster Recovery group

Beginning with ONTAP 9.8, you can remove a DR group from an eight-node MetroCluster configuration to create a four-node MetroCluster configuration.

This procedure is supported on ONTAP 9.8 and later. On earlier versions of ONTAP, please contact technical support to remove a DR group.

[NetApp Support](#)

An eight-node configuration includes eight-nodes organized as two four-node DR groups.



By removing a DR Group, four nodes remain in the configuration.



Removing the DR group nodes from each cluster

- You must perform this step on both clusters.
- The `metrocluster remove-dr-group` command is supported only on ONTAP 9.8 and later.
 1. Prepare for the removal of the DR group, if you haven't already.
 - a. Move all data volumes to another DR group.

- b. Move all MDV_CRS metadata volumes to another DR group. Follow the steps in the following procedure: [Moving a metadata volume in MetroCluster configurations](#)
- c. Delete all MDV_aud metadata volumes that might exist in the DR group to be removed.
- d. Delete all data aggregates in the DR group to be removed as shown in the following example:

```
ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
-fields aggregate ,node
ClusterA::> aggr delete -aggregate aggregate_name
ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
-fields aggregate ,node
ClusterB::> aggr delete -aggregate aggregate_name
```



Root aggregates are not deleted.

- e. Migrate all data LIFs to home nodes in another DR group.

```
network interface show -home-node old_node
```

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

- f. Migrate the cluster management LIF to a home node in another DR group.

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

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

Node management and inter-cluster LIFs are not migrated.

- g. Transfer epsilon to a node in another DR group if required.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identify and remove the DR group.

- a. Identify the correct DR group for removal:

```
metrocluster node show
```

- b. Remove the DR group nodes:

```
metrocluster remove-dr-group -dr-group-id 1
```

The following example shows the removal of the DR group configuration on cluster_A.

```
cluster_A::*>
```

Warning: Nodes in the DR group that are removed from the MetroCluster

configuration will lose their disaster recovery protection.

Local nodes "node_A_1-FC, node_A_2-FC" will be removed from the

MetroCluster configuration. You must repeat the operation on the

partner cluster "cluster_B" to remove the remote nodes in the DR group.

Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and partner

clusters before removing a DR group.

1. Move all data volumes to another DR group.
2. Move all MDV_CRS metadata volumes to another DR group.
3. Delete all MDV_aud metadata volumes that may exist in the DR group to be removed.
4. Delete all data aggregates in the DR group to be removed.

Root

aggregates are not deleted.

5. Migrate all data LIFs to home nodes in another DR group.
6. Migrate the cluster management LIF to a home node in another DR group.

Node management and inter-cluster LIFs are not migrated.

7. Transfer epsilon to a node in another DR group.

The command is vetoed if the preparation steps are not completed on the

local and partner clusters.

Do you want to continue? {y|n}: y

[Job 513] Job succeeded: Remove DR Group is successful.

```
cluster_A::*>
```

3. Repeat the previous step on the partner cluster.
4. If in a MetroCluster IP configuration, remove the MetroCluster connections on the nodes of the old DR group.

These commands can be issued from either cluster and apply to the entire DR group spanning both the clusters.

- a. Disconnect the connections:

```
metrocluster configuration-settings connection disconnect dr-group-id
```

- b. Delete the MetroCluster interfaces on the nodes of the old DR group:

```
metrocluster configuration-settings interface delete
```

- c. Delete the old DR group's configuration.

```
metrocluster configuration-settings dr-group delete
```

5. Unjoin the nodes in the old DR group.

You must perform this step on each cluster.

- a. Set the advanced privilege level:

```
set -privilege advanced
```

- b. Disable the storage failover:

```
storage failover modify -node node-name -enable false ←-----Additional  
step
```

- c. Unjoin the node:

```
cluster unjoin -node node-name
```

Repeat this step for the other local node in the old DR group.

- d. Set the admin privilege level:

```
set -privilege admin
```

6. Re-enable cluster HA in the new DR group:

```
cluster ha modify -configured true
```

You must perform this step on each cluster.

7. Halt, power down, and remove the old controller modules and storage shelves.


Where to find additional information

You can learn more about MetroCluster configuration and operation.

MetroCluster and miscellaneous information

Information	Subject
MetroCluster Documentation	<ul style="list-style-type: none">• All MetroCluster information

Fabric-attached MetroCluster installation and configuration	<ul style="list-style-type: none"> • Fabric-attached MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the FC switches • Configuring the MetroCluster in ONTAP
Stretch MetroCluster installation and configuration	<ul style="list-style-type: none"> • Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP
MetroCluster management and disaster recovery	<ul style="list-style-type: none"> • Understanding the MetroCluster configuration • Switchover, healing and switchback • Disaster recovery
Maintain MetroCluster Components	<ul style="list-style-type: none"> • Guidelines for maintenance in a MetroCluster FC configuration • Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration • Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration.
MetroCluster Upgrade, Transition, and Expansion	<ul style="list-style-type: none"> • Upgrading or refreshing a MetroCluster configuration • Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration • Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Tiebreaker Software installation and configuration	<ul style="list-style-type: none"> • Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software

<p>AFF and FAS Documentation Center</p> <div data-bbox="167 205 220 262">  </div> <p>The standard storage shelf maintenance procedures can be used with MetroCluster IP configurations.</p>	<ul style="list-style-type: none"> • Hot-adding a disk shelf • Hot-removing a disk shelf
<p>Copy-based transition</p>	<ul style="list-style-type: none"> • Transitioning data from 7-Mode storage systems to clustered storage systems
<p>ONTAP concepts</p>	<ul style="list-style-type: none"> • How mirrored aggregates work

Copyright Information

Copyright © 2022 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.