



Transition from MetroCluster FC to MetroCluster IP

ONTAP MetroCluster

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-metrocluster/transition/concept_choosing_your_transition_procedure_mcc_transition.html on February 13, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Transition from MetroCluster FC to MetroCluster IP	1
Choose your transition procedure	1
Supported platform combinations	1
Choose your transition procedure	3
Transition nondisruptively from a MetroCluster FC to a MetroCluster IP configuration (ONTAP 9.8 and later)	4
Transitioning nondisruptively from a MetroCluster FC to a MetroCluster IP configuration (ONTAP 9.8 and later)	4
Prepare for transition from a MetroCluster FC to a MetroCluster IP configuration	5
Transition from MetroCluster FC to MetroCluster IP configurations	16
Sending a custom AutoSupport message after maintenance	70
Restoring Tiebreaker or Mediator monitoring	70
Disruptively transition from a two-node MetroCluster FC to a four-node MetroCluster IP configuration (ONTAP 9.8 and later)	70
Disruptively transitioning from a two-node MetroCluster FC to a four-node MetroCluster IP configuration (ONTAP 9.8 and later)	70
Example naming in this procedure	71
Preparing for disruptive FC-to-IP transition	72
Transitioning the MetroCluster FC nodes	81
Connecting the MetroCluster IP controller modules	90
Configuring the new nodes and completing transition	106
Returning the system to normal operation	111
Disruptively transitioning from MetroCluster FC to MetroCluster IP when retiring storage shelves (ONTAP 9.8 and later)	113
Enable console logging	113
Requirements for transition when retiring old shelves	114
Workflow for disruptive transition when moving data and retiring old storage shelves	114
Transitioning the configuration	115
Migrating the root aggregates	116
Migrating the data aggregates	117
Retiring shelves moved from node_A_1-FC and node_A_2-FC	117
Completing transition	118
Disruptively transitioning when existing shelves are not supported on new controllers (ONTAP 9.8 and later)	119
Enable console logging	119
Requirements for transition when shelves are not supported on the new nodes	119
Workflow for disruptive transition when shelves are not supported by new controllers	120
Preparing the new controller modules	121
Attaching the new disk shelves to the existing MetroCluster FC controllers	121
Migrate root aggregates and move data to the new disk shelves	122
Transitioning the configuration	128
Moving an FC SAN workload from MetroCluster FC to MetroCluster IP nodes	129
Move an FC SAN workload from MetroCluster FC to MetroCluster IP nodes	129

Move Linux iSCSI hosts from MetroCluster FC to MetroCluster IP nodes	136
Step 1: Set up new iSCSI connections	136
Step 2: Add the new nodes as reporting nodes	140
Step 3: Remove reporting nodes and rescan paths	145
Where to find additional information	147
MetroCluster and miscellaneous information	147

Transition from MetroCluster FC to MetroCluster IP

Choose your transition procedure

When transitioning to a MetroCluster IP configuration, you must have a combination of supported platform models.

You should also ensure that the MetroCluster IP platform is an appropriate size for the load that you are transitioning from the MetroCluster FC configuration to the MetroCluster IP configuration.

Supported platform combinations

- The transition procedures all require ONTAP 9.8 or later unless stated otherwise in the notes or as required by an individual platform.
- All nodes in the MetroCluster configuration must be running the same ONTAP version. For example, if you have an eight-node configuration, all eight nodes must be running the same ONTAP version. Refer to the [Hardware universe](#) for the minimum supported ONTAP version for your combination.
 - Do not exceed any object limits of the 'lower' of the platforms in the combination. Apply the lower object limit of the two platforms.
 - If the target platform limits are lower than the MetroCluster limits, you must reconfigure the MetroCluster to be at, or below, the target platform limits before you add the new nodes.
 - Refer to the [Hardware universe](#) for platform limits.

Supported AFF and FAS transition combinations

The following tables show the supported platform combinations. You can transition from platforms in the first column to platforms listed as supported in the columns to the right, as indicated by the colored table cells.

For example, transitioning from a MetroCluster FC configuration consisting of AFF8060 controller modules to an IP configuration consisting of AFF A400 controller modules is supported.

The tables are split into two groups:

- **Group 1** shows combinations for transitions to AFF A150, AFF A20, FAS2750, AFF A220, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A320, FAS8300, AFF C400, AFF A400, and FAS8700 systems.
- **Group 2** shows combinations for transitions to AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90, and AFF A1K systems.

The following notes apply to both groups:

- Note 1: This platform combination requires ONTAP 9.11.1 or later.
- Note 2: You must have a 40GbE interface for the local cluster interfaces on the FC nodes.
- Note 3: You must have a 100GbE interface for the local cluster interfaces on the FC nodes.

AFF and FAS combinations group 1

Review the supported combinations for transitions to AFF A150, AFF A20, FAS2750, AFF A220, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A320, FAS8300, AFF C400, AFF A400, and FAS8700 systems.

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300				Note 1						
	FAS8300 AFF A400										
	FAS9000 AFF A700										
	FAS9500 AFF A900										

AFF and FAS combinations group 2

Review the supported combinations for transitions to AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90, and AFF A1K systems.

AFF and FAS		Target MetroCluster IP platform									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300										
	FAS8300 AFF A400										
	FAS9000 AFF A700			Note 2	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2	
	FAS9500 AFF A900							Note 3	Note 3	Note 3	Note 3

Supported ASA transition platform combinations

The following table shows the supported platform combinations for ASA systems.

Source MetroCluster FC platform	Target MetroCluster IP platform	Supported?
ASA A400	ASA A400	Yes
	ASA A900	No
ASA A900	ASA A400	No
	ASA A900	Yes

Choose your transition procedure

You must select a transition procedure depending on your existing MetroCluster FC configuration.

A transition procedure replaces the back-end FC switch fabric or FC-VI connection with an IP switch network. The exact procedure depends on your starting configuration.

The original platforms and FC switches (if present) are retired at the end of the transition procedure.

Starting configuration	Disruptive or nondisruptive	Requirements	Procedure
Four or eight node	Nondisruptive	New storage shelves are required on new platforms. After the transition is completed, old controllers, shelves and disks are removed from the cluster.	Link to procedure Note: This procedure supports the following FC to IP transitions: <ul style="list-style-type: none"> From a four-node MetroCluster FC configuration to a four-node MetroCluster IP configuration From an eight-node MetroCluster FC configuration to an eight-node MetroCluster IP configuration
Two node	Disruptive	New storage shelves are supported on both original and new platforms.	Link to procedure
Two node	Disruptive	New storage shelves are supported on both original and new platforms. Old storage shelves must be retired.	Link to procedure
Two node	Disruptive	Old storage shelves are not supported on new platforms. Old storage shelves must be retired.	Link to procedure

Transition nondisruptively from a MetroCluster FC to a MetroCluster IP configuration (ONTAP 9.8 and later)

Transitioning nondisruptively from a MetroCluster FC to a MetroCluster IP configuration (ONTAP 9.8 and later)

You can perform nondisruptive transitions of workloads and data from an existing MetroCluster FC configuration to a new MetroCluster IP configuration.

Beginning with ONTAP 9.13.1, this procedure is supported in MetroCluster IP configurations in which the MetroCluster and the drive shelves are connected to the same IP switches (a shared storage switch configuration).

Beginning with ONTAP 9.13.1, you can perform a nondisruptive transition of workloads and data from an existing eight-node MetroCluster FC configuration to a new eight-node MetroCluster IP configuration. You use this procedure to transition one four-node FC DR group, remove the empty FC DR group, and then repeat the procedure for the second FC DR group.

Beginning with ONTAP 9.8, you can perform a nondisruptive transition of workloads and data from an existing four-node MetroCluster FC configuration to a new four-node MetroCluster IP configuration. After you complete the transition, you can expand to an eight-node MetroCluster IP configuration if required. See [Expand a MetroCluster IP configuration](#).

- This procedure is nondisruptive.

The MetroCluster configuration can continue to serve data during the operation.

- This procedure applies only to four-node and eight-node MetroCluster FC configurations.

If you have a two-node MetroCluster FC configuration, see [Choosing your transition procedure](#).

- This procedure describes the steps required to transition one four-node FC DR group. If you have an eight-node configuration (two FC DR groups), you must repeat the entire procedure for each FC DR group.



When you add or remove a DR group as part of this procedure, you must verify that the DR group removal or addition was successful before adding or removing another DR group.

- You must meet all requirements and follow all steps in the procedure.

Important information if you are adding an older platform model

The following guidance is for an uncommon scenario where you need to add an older platform model (platforms released before ONTAP 9.15.1) to an existing MetroCluster configuration that contains a newer platform model (platforms released in ONTAP 9.15.1 or later). For an eight-node FC to IP transition, this guidance applies if you have transitioned your first FC DR group to a platform model introduced in ONTAP 9.15.1 or later and plan to transition the second DR group to a platform introduced before ONTAP 9.15.1.

If your existing MetroCluster configuration contains a platform that uses **shared cluster/HA ports** (platforms released in ONTAP 9.15.1 or later), you cannot add a platform that uses **shared MetroCluster/HA ports** (platforms released before ONTAP 9.15.1) without upgrading all nodes in the configuration to ONTAP 9.15.1P11 or ONTAP 9.16.1P4 or later.



Adding an older platform model that uses **shared/MetroCluster HA ports** to a MetroCluster containing a newer platform model that uses **shared cluster/HA ports** is an uncommon scenario and most combinations are not affected.

Use the following table to verify whether your combination is affected. If your existing platform is listed in the first column, and the platform you want to add to the configuration is listed in the second column, all nodes in the configuration must be running ONTAP 9.15.1P11 or ONTAP 9.16.1P4 or later to add the new DR group.

If your existing MetroCluster contains..	And the platform you're adding is...	Then...
An AFF system using shared cluster/HA ports : <ul style="list-style-type: none">• AFF A20• AFF A30• AFF C30• AFF A50• AFF C60• AFF C80• AFF A70• AFF A90• AFF A1K	A FAS system using shared cluster/HA ports : <ul style="list-style-type: none">• FAS50• FAS70• FAS90 An AFF system using shared MetroCluster/HA ports : <ul style="list-style-type: none">• AFF A150, ASA A150• AFF A220• AFF C250, ASA C250• AFF A250, ASA A250• AFF A300• AFF A320• AFF C400, ASA C400• AFF A400, ASA A400• AFF A700• AFF C800, ASA C800• AFF A800, ASA A800• AFF A900, ASA A900	A FAS system using shared MetroCluster/HA ports : <ul style="list-style-type: none">• FAS2750• FAS500f• FAS8200• FAS8300• FAS8700• FAS9000• FAS9500 Before you add the new platform to your existing MetroCluster configuration, upgrade all nodes in the existing and new configuration to ONTAP 9.15.1P11 or ONTAP 9.16.1P4 or later.

Prepare for transition from a MetroCluster FC to a MetroCluster IP configuration

Enable console logging

Enable console logging on your devices before performing this task.

NetApp strongly recommends that you enable console logging on the devices that you are using and take the following actions when performing this procedure:

- Leave AutoSupport enabled during maintenance.
- Trigger a maintenance AutoSupport message before and after maintenance to disable case creation for the

duration of the maintenance activity.

See the Knowledge Base article [How to suppress automatic case creation during scheduled maintenance windows](#).

- Enable session logging for any CLI session. For instructions on how to enable session logging, review the "Logging Session Output" section in the Knowledge Base article [How to configure PuTTY for optimal connectivity to ONTAP systems](#).

Requirements for nondisruptive FC-to-IP transition

Before starting the transition process, verify that the configuration meets the requirements.

You can perform a nondisruptive FC-to-IP transition if your configuration meets the following requirements:

- If you have an eight-node configuration, all nodes are running ONTAP 9.13.1 or later.
- If you have a four-node configuration, all nodes are running ONTAP 9.8 or later.
- The existing and new platforms are a supported combination for transition.

Supported platforms for nondisruptive transition

- Your configuration supports a switched cluster configuration.

Hardware Universe

 If you are using shared storage MetroCluster switches, you can only transition to a four-node MetroCluster IP configuration. Transitioning to an eight-node MetroCluster IP configuration using shared storage MetroCluster switches is not supported. After you complete the transition to a four-node MetroCluster IP configuration, you can [expand to an eight-node MetroCluster IP configuration](#).

- Your configuration meets all requirements and is cabled as described in the following *MetroCluster Installation and Configuration* procedures.

Fabric-attached MetroCluster installation and configuration

Stretch MetroCluster installation and configuration

How transition impacts the MetroCluster hardware components

After completing the transition procedure, key components of the existing MetroCluster configuration have been replaced or reconfigured.

- **Controller modules**

The existing controller modules are replaced by new controller modules. The existing controller modules are decommissioned at the end of the transition procedures.

- **Storage shelves**

Data is moved from the old shelves to the new shelves. The old shelves are decommissioned at the end of

the transition procedures.

- **MetroCluster (back-end) and cluster switches**

The back-end switch functionality is replaced by the IP switch fabric. If the MetroCluster FC configuration included FC switches and FC-to-SAS bridges, they are decommissioned at the end of this procedure.

If the MetroCluster FC configuration used cluster switches for the cluster interconnect, in some cases they can be reused to provide the back-end IP switch fabric. Reused cluster switches must be reconfigured with platform and switch-specific RCFs. procedures.

If the MetroCluster FC configuration did not use cluster switches, new IP switches are added to provide the backend switch fabric.

[Considerations for IP switches](#)

- **Cluster peering network**

The existing customer-provided cluster peering network can be used for the new MetroCluster IP configuration. Cluster peering is configured on the MetroCluster IP nodes as part of the transition procedure.

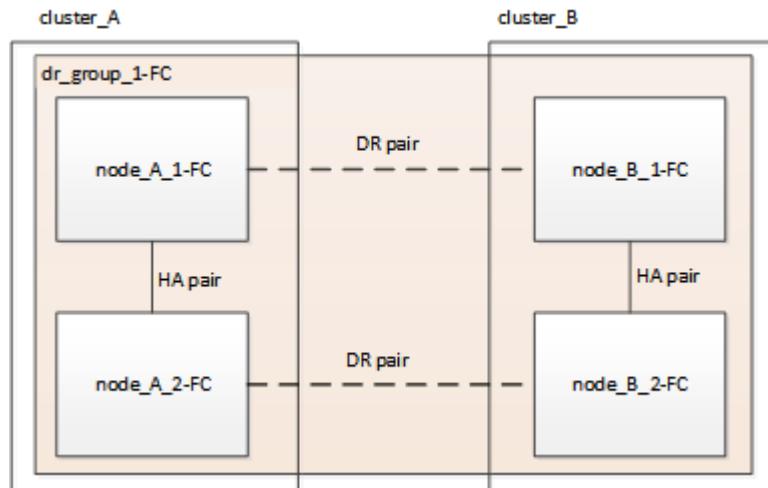
Workflow for nondisruptive MetroCluster transition

You must follow the specific workflow to ensure a successful nondisruptive transition. Choose the workflow for your configuration:

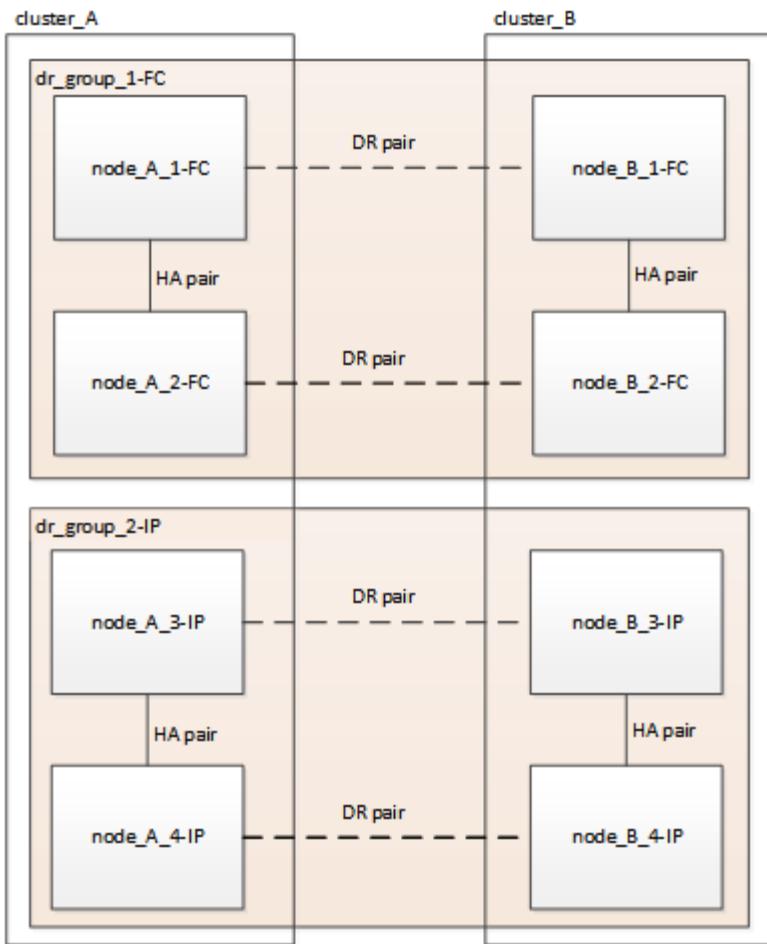
- [Four-node FC configuration transition workflow](#)
- [Eight-node FC configuration transition workflow](#)

Four-node FC configuration transition workflow

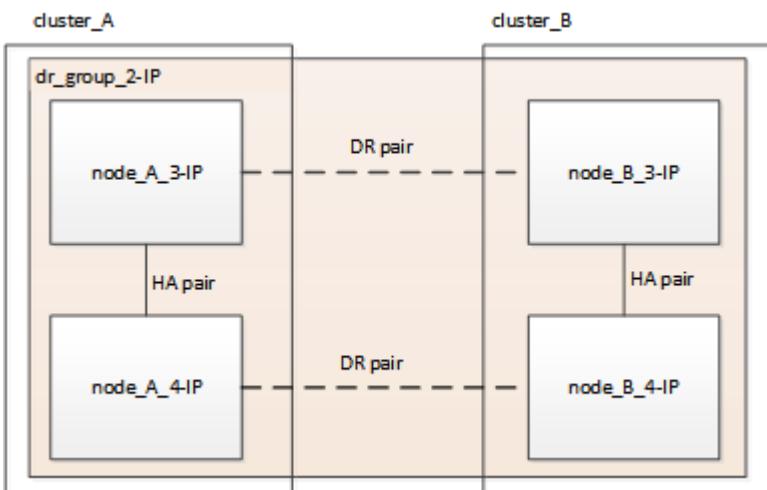
The transition process begins with a healthy four-node MetroCluster FC configuration.



The new MetroCluster IP nodes are added as a second DR group.

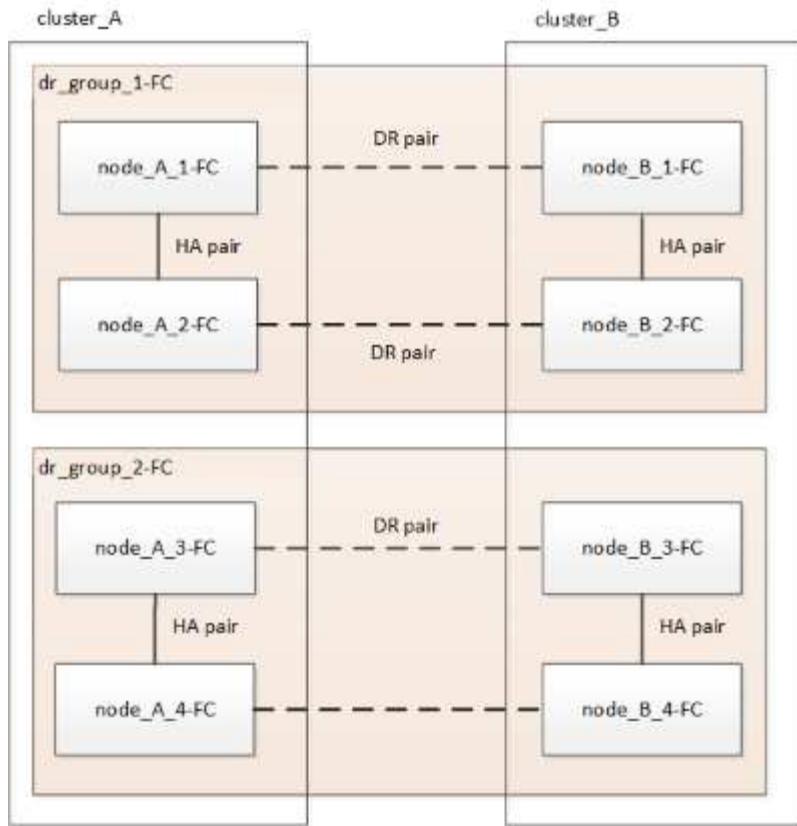


Data is transferred from the old DR group to the new DR group, and then the old nodes and their storage are removed from the configuration and decommissioned. The process ends with a four-node MetroCluster IP configuration.

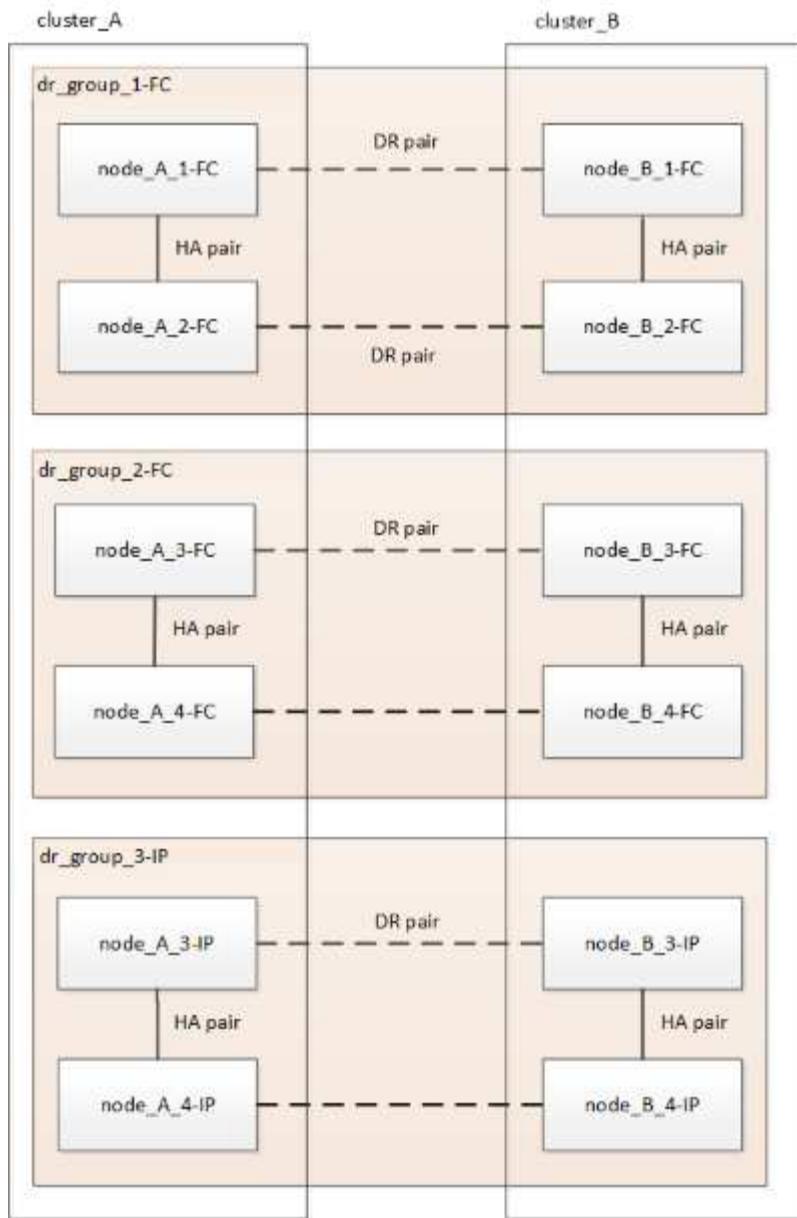


Eight-node FC configuration transition workflow

The transition process begins with a healthy eight-node MetroCluster FC configuration.



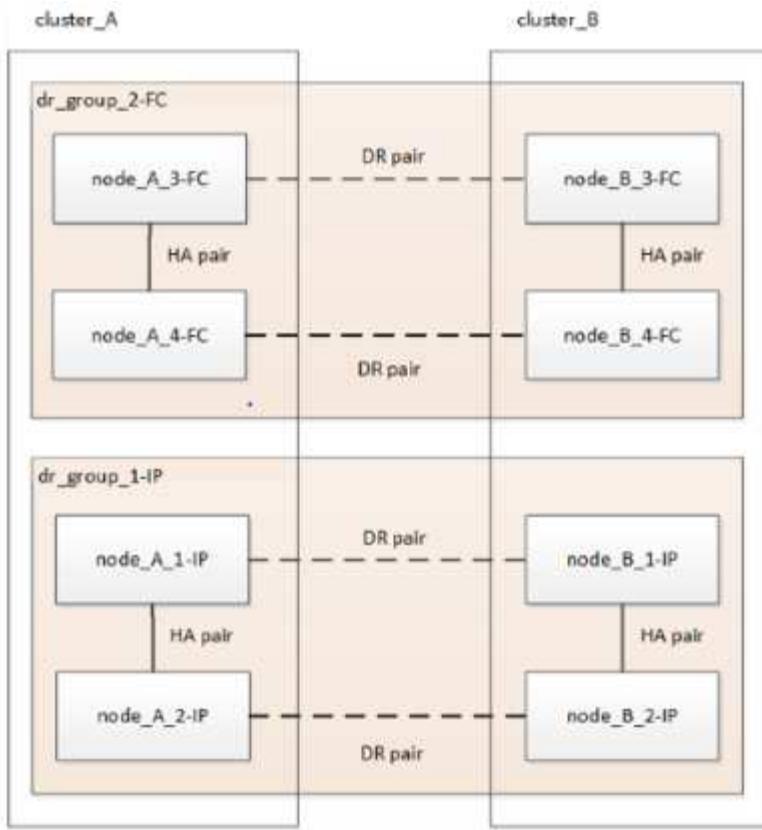
The new MetroCluster IP nodes are added as a third DR group.



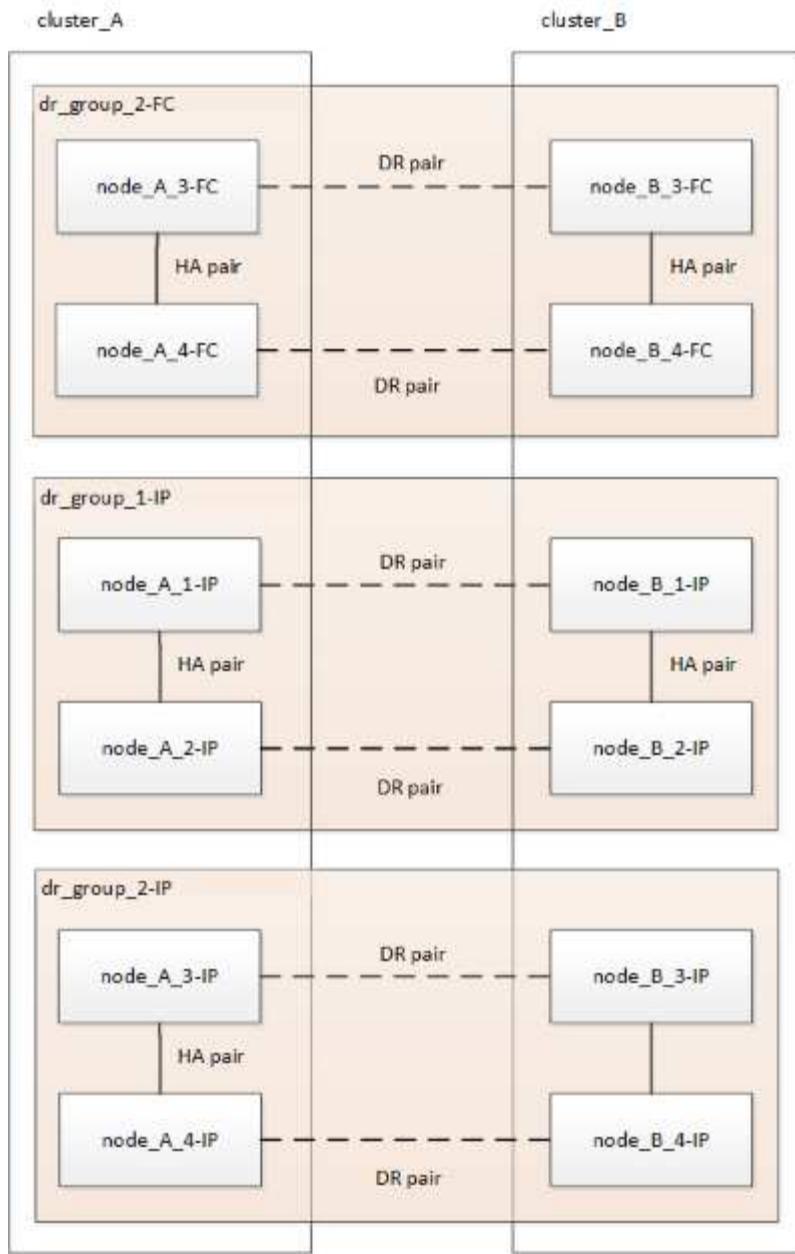
Data is transferred from DR_group_1-FC to DR_group_1-IP, and then the old nodes and their storage are removed from the configuration and decommissioned.



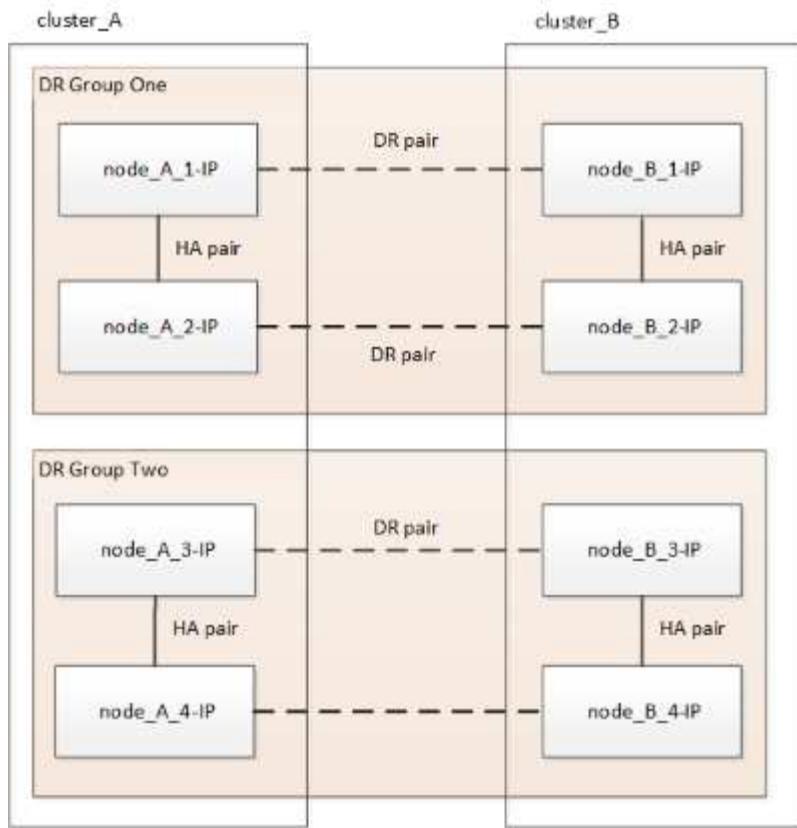
If you want to transition from an eight-node FC configuration to a four-node IP configuration, you must transition all the data in DR_group_1-FC and DR_group_2-FC to the new IP DR group (DR_group_1-IP). You can then decommission both FC DR groups. After the FC DR groups have been removed, the process ends with a four-node MetroCluster IP configuration.



Add the remaining MetroCluster IP nodes to the existing MetroCluster configuration. Repeat the process to transfer data from the DR_group_2-FC nodes to the DR_group_2-IP nodes.

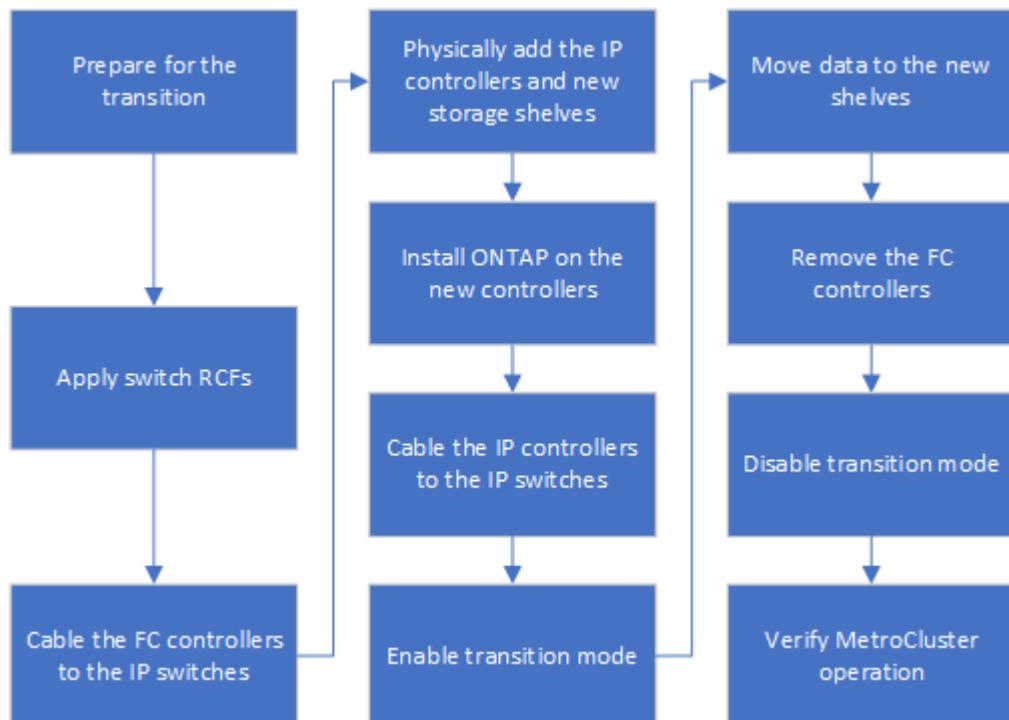


After removing DR_group_2-FC, the process ends with an eight-node MetroCluster IP configuration.



Transition process workflow

You will use the following workflow to transition the MetroCluster configuration.



Considerations for IP switches

You must ensure the IP switches are supported. If the existing switch model is supported

by both the original MetroCluster FC configuration and the new MetroCluster IP configuration, you can reuse the existing switches.

Supported switches

You must use NetApp-provided switches.

- The use of MetroCluster-compliant switches (switches that are not validated and provided by NetApp) is not supported for transition.
- The IP switches must be supported as a cluster switch by both the MetroCluster FC configuration and the MetroCluster IP configuration.
- The IP switches can be reused in the new MetroCluster IP configuration if the MetroCluster FC is a switched cluster and the IP cluster switches are supported by the MetroCluster IP configuration.
- New IP switches are usually used in the following cases:
 - The MetroCluster FC is a switchless cluster, so new switches are required.
 - The MetroCluster FC is a switched cluster but the existing IP switches are not supported in the MetroCluster IP configuration.
 - You want to use different switches for the MetroCluster IP configuration.

 If you are using shared storage MetroCluster switches, you can only transition to a four-node MetroCluster IP configuration. Transitioning to an eight-node MetroCluster IP configuration using shared storage MetroCluster switches is not supported. After you complete the transition to a four-node MetroCluster IP configuration, you can [expand to an eight-node MetroCluster IP configuration](#).

See the [Hardware Universe](#) for information on platform models and switch support.

Switchover, healing, and switchback operations during nondisruptive transition

Depending on the stage of the transition process, the MetroCluster switchover, healing, and switchback operations use either the MetroCluster FC or MetroCluster IP workflow.

The following table shows what workflows are used at different stages of the transition process. In some stages, switchover and switchback are not supported.

- In the MetroCluster FC workflow, the switchover, healing, and switchback steps are those used by a MetroCluster FC configuration.
- In the MetroCluster IP workflow, the switchover, healing, and switchback steps are those used by a MetroCluster IP configuration.
- In the unified workflow, when both the FC and IP nodes are configured, the steps depend on whether NSO or USO is performed. The details are shown in the table.

For information on the MetroCluster FC and IP workflows for switchover, healing, and switchback, see [Understanding MetroCluster data protection and disaster recovery](#).



Automatic unplanned switchover is not available during the transition process.

Stage of transition	Negotiated switchover uses this workflow...	Unplanned switchover uses this workflow...
Before the MetroCluster IP nodes have joined the cluster	MetroCluster FC	MetroCluster FC
After the MetroCluster IP nodes have joined the cluster, before the <code>metrocluster configure</code> command is performed	Not supported	MetroCluster FC
After the <code>metrocluster configure</code> command has been issued. Volume move can be in progress.	Unified: All remote site nodes remain up and healing is done automatically	Unified: <ul style="list-style-type: none"> Mirrored aggregates owned by the MetroCluster FC node are mirrored if storage is accessible, all others are degraded after switchover. All remote site nodes are able to boot up. The <code>heal aggregate</code> and <code>heal root</code> commands must be run manually.
The MetroCluster FC nodes have been unconfigured.	Not supported	MetroCluster IP
The <code>cluster unjoin</code> command has been performed on the MetroCluster FC nodes.	MetroCluster IP	MetroCluster IP

Alert messages and tool support during transition

You may notice alert messages during transition. These alerts can be safely ignored. Also, some tools are not available during transition.

- ARS may alert during transition.

These alerts can be ignored and should disappear once the transition has finished.

- OnCommand Unified Manager may alert during transition.

These alerts can be ignored and should disappear once the transition has finished.

- Config Advisor is not supported during transition.
- System Manager is not supported during transition.

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-FC	<ul style="list-style-type: none"> • node_A_1-FC • node_A_2-FC 	<ul style="list-style-type: none"> • node_B_1-FC • node_B_2-FC
dr_group_2-IP	<ul style="list-style-type: none"> • node_A_3-IP • node_A_4-IP 	<ul style="list-style-type: none"> • node_B_3-IP • node_B_4-IP
Switches	Initial switches (if fabric-attached configuration:) <ul style="list-style-type: none"> • switch_A_1-FC • switch_A_2-FC MetroCluster IP switches: <ul style="list-style-type: none"> • switch_A_1-IP • switch_A_2-IP 	Initial switches (if fabric-attached configuration:) <ul style="list-style-type: none"> • switch_B_1-FC • switch_B_2-FC MetroCluster IP switches: <ul style="list-style-type: none"> • switch_B_1-IP • switch_B_2-IP

Transition from MetroCluster FC to MetroCluster IP configurations

Verifying the health of the MetroCluster configuration

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

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. Check for any health alerts on the switches (if present): `storage switch show`
 - g. Run Config Advisor.

[NetApp Downloads: Config Advisor](#)

 - h. 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`

```
cluster_A::> cluster show
Node          Health  Eligibility  Epsilon
-----  -----  -----  -----
node_A_1_FC   true    true        false
node_A_2_FC   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_FC

          Speed (Mbps)  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
-----  -----  -----  -----
e0a      Cluster      Cluster          up    9000  auto/10000 healthy
e0b      Cluster      Cluster          up    9000  auto/10000 healthy

Node: node_A_2_FC

          Speed (Mbps)  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
-----  -----  -----  -----
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 "up/up" for "Status Admin/Oper".

```

cluster_A::> network interface show -vserver cluster

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

-----
----- Cluster
          node_A-1_FC_clus1
          up/up      169.254.209.69/16  node_A-1_FC  e0a
true
          node_A_1_FC_clus2
          up/up      169.254.49.125/16  node_A_1_FC  e0b
true
          node_A_2_FC_clus1
          up/up      169.254.47.194/16  node_A_2_FC  e0a
true
          node_A_2_FC_clus2
          up/up      169.254.19.183/16  node_A_2_FC  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_FC_clus1
                  true
      node_A_1_FC_clus2
                  true
      node_A_2_FC_clus1
                  true
      node_A_2_FC_clus2
                  true

4 entries were displayed.

cluster_A::>

```

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.

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.

Generating and applying RCFs to the new IP switches

If you are using new IP switches for the MetroCluster IP configuration, you must configure the switches with a custom RCF file.

This task is required if you are using new switches.

If you are using existing switches, proceed to [Moving the local cluster connections](#).

1. Install and rack the new IP switches.
2. Prepare the IP switches for the application of the new RCF files.

Follow the steps in the section for your switch vendor:

- Reset the Broadcom IP switch to factory defaults
- Reset the Cisco IP switch to factory defaults
- Reset the NVIDIA IP SN2100 switch to factory defaults

3. Update the firmware on the switch to a supported version, if necessary.

4. Use the RCF generator tool to create the RCF file depending on your switch vendor and the platform models, and then update the switches with the file.

Follow the steps in the section for your switch vendor:

- Download and install the Broadcom IP RCF files
- Download and install the Cisco IP RCF files
- Download and install the NVIDIA RCF files

Move the local cluster connections

Move the MetroCluster FC configuration's cluster interfaces to the IP switches.

Step 1: Move the cluster connections on the MetroCluster FC nodes

Move the cluster connections on the MetroCluster FC nodes to the IP switches. The steps you follow depend on whether you're using existing IP switches or new IP switches.

About this task

- You perform this task on both MetroCluster sites.

Which connections to move

The following task assumes a controller module is using two ports for the cluster connections. Some controller module models use four or more ports for the cluster connection. In this example, the ports are divided into two groups, alternating ports between the two groups.

The following table shows the example ports used in this task.

Number of cluster connections on the controller module	Group A ports	Group B ports
Two	e0a	e0b
Four	e0a, e0c	e0b, e0d

- Group A ports connect to local switch switch_x_1-IP.
- Group B ports connect to local switch switch_x_2-IP.

The following table shows which switch ports the FC nodes connect to. For the Broadcom BES-53248 switch, the port usage depends on the model of the MetroCluster IP nodes.

Switch model	MetroCluster IP node model	Switch port(s)	Connects to

Cisco 3132Q-V	Any	5, 6	Local cluster interface on FC node
Cisco 9336C-FX2 (12-port)	Any	3,4, or 11,12 Note: To use switch ports 11 and 12, you must select two speed modes.	Local cluster interface on FC node
Cisco 3232C, or 9336C-FX2 (36-port)	Any	5, 6, or 13, 14 Note: To use switch ports 13 and 14, you must select two speed modes.	Local cluster interface on FC node
Cisco 9336C-FX2 shared (36-port)	Any	3,4, or 11,12 Note: To use switch ports 11 and 12, you must select two speed modes.	Local cluster interface on FC node
Broadcom BES-53248	FAS500f/A250	1 - 6	Local cluster interface on FC node
	FAS8200/A300	3, 4, 9, 10, 11, 12	Local cluster interface on FC node
	FAS8300/A400/FAS8700	1 - 6	Local cluster interface on FC node
NVIDIA SN2100	Any	5,6, or 11,12 Note: To use switch ports 11 and 12, you must select two speed modes.	Local cluster interface on FC node

Move the local cluster connections when using new IP switches

If you are using new IP switches, you physically move the existing MetroCluster FC nodes' cluster connections to the new switches.

Steps

1. Move the MetroCluster FC node group A cluster connections to the new IP switches.

Use the ports described in [Which connections to move](#).

- a. Disconnect all the group A ports from the switch, or, if the MetroCluster FC configuration was a switchless cluster, disconnect them from the partner node.
- b. Disconnect the group A ports from node_A_1-FC and node_A_2-FC.

- c. Connect the group A ports of node_A_1-FC to the switch ports for the FC node on switch_A_1-IP
- d. Connect the group A ports of node_A_2-FC to the switch ports for the FC node on switch_A_1-IP

2. Verify that all cluster ports are up:

```
network port show -ipspace Cluster
```

```
cluster_A::*> network port show -ipspace Cluster
```

```
Node: node_A_1-FC
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps)	Health	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy		
e0b	Cluster	Cluster		up	9000	auto/10000	healthy		

```
Node: node_A_2-FC
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps)	Health	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy		
e0b	Cluster	Cluster		up	9000	auto/10000	healthy		

```
4 entries were displayed.
```

```
cluster_A::*>
```

3. Verify that your inter-site Inter-Switch Links (ISLs) are up and the port-channels are operational:

```
show interface brief
```

In the following example, ISL ports “Eth1/15” to “Eth1/20” are configured as “Po10” for the remote site link and “Eth1/7” to “Eth1/8” are configured as “Po1” for the local cluster ISL. The state of “Eth1/15” to “Eth1/20”, “Eth1/7” to “Eth1/8”, “Po10”, and “Po1” should be ‘up’.

```
IP_switch_A_1# show interface brief
```

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	100.10.200.20	1000	1500

Ethernet Port	VLAN	Type	Mode	Status	Reason	Speed
---------------	------	------	------	--------	--------	-------

Interface	Ch #
---	---
...	
Eth1/7 1	1 eth trunk up none 100G (D)
Eth1/8 1	1 eth trunk up none 100G (D)
...	
Eth1/15 10	1 eth trunk up none 100G (D)
Eth1/16 10	1 eth trunk up none 100G (D)
Eth1/17 10	1 eth trunk up none 100G (D)
Eth1/18 10	1 eth trunk up none 100G (D)
Eth1/19 10	1 eth trunk up none 100G (D)
Eth1/20 10	1 eth trunk up none 100G (D)
---	---
Port-channel Interface	

Po1	1 eth trunk up none a-100G (D) lacp
Po10	1 eth trunk up none a-100G (D) lacp
Po11	1 eth trunk down No operational auto (D) lacp members
IP_switch_A_1#	

4. Verify that all interfaces display true in the “Is Home” column:

```
network interface show -vserver cluster
```

This might take several minutes to complete.

```

cluster_A::*> network interface show -vserver cluster

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

-----
----- Cluster
          node_A_1_FC_clus1
          up/up      169.254.209.69/16  node_A_1_FC  e0a
true
          node_A_1-FC_clus2
          up/up      169.254.49.125/16  node_A_1-FC  e0b
true
          node_A_2-FC_clus1
          up/up      169.254.47.194/16  node_A_2-FC  e0a
true
          node_A_2-FC_clus2
          up/up      169.254.19.183/16  node_A_2-FC  e0b
true

4 entries were displayed.

cluster_A::*>

```

5. Perform the above steps on both nodes (node_A_1-FC and node_A_2-FC) to move the group B ports of the cluster interfaces.
6. Repeat the above steps on the partner cluster “cluster_B”.

Move the local cluster connections when reusing existing IP switches

If you are reusing existing IP switches, you update firmware, reconfigure the switches with the correct reference configuration files (RCFs) and move the connections to the correct ports one switch at a time.

About this task

This task is required only if the FC nodes are connected to existing IP switches and you are reusing the switches.

Steps

1. Disconnect the local cluster connections that connect to switch_A_1_IP
 - a. Disconnect the group A ports from the existing IP switch.
 - b. Disconnect the ISL ports on switch_A_1_IP.

You can see the Installation and Setup instructions for the platform to see the cluster port usage.

[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](#)

2. Reconfigure switch_A_1_IP using RCF files generated for your platform combination and transition.

Follow the steps in the procedure for your switch vendor from *MetroCluster IP Installation and Configuration*:

[MetroCluster IP installation and configuration](#)

a. If required, download and install the new switch firmware.

You should use the latest firmware that the MetroCluster IP nodes support.

- [Download and install the Broadcom switch EFOS software](#)
- [Download and install the Cisco switch NX-OS software](#)
- [Download and install the NVIDIA Cumulus software](#)

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

- [Reset the Broadcom IP switch to factory defaults](#)
- [Reset the Cisco IP switch to factory defaults](#)
- [Reset the NVIDIA IP SN2100 switch to factory defaults](#)

c. Download and install the IP RCF file depending on your switch vendor.

- [Download and installing the Broadcom IP RCF files](#)
- [Download and installing the Cisco IP RCF files](#)
- [Download and install the NVIDIA RCF files](#)

3. Reconnect the group A ports to switch_A_1_IP.

Use the ports described in [Which connections to move](#).

4. Verify that all cluster ports are up:

```
network port show -ipspace cluster
```

```
Cluster-A::*> network port show -ipspace cluster
```

```
Node: node_A_1_FC
```

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps)	Health
					Admin/Oper	Status
e0a	Cluster	Cluster	up	9000	auto/10000	healthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy

```
Node: node_A_2_FC
```

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps)	Health
					Admin/Oper	Status
e0a	Cluster	Cluster	up	9000	auto/10000	healthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy

```
4 entries were displayed.
```

```
Cluster-A::*>
```

5. Verify that all interfaces are on their home port:

```
network interface show -vserver Cluster
```

```

Cluster-A::*> network interface show -vserver Cluster

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

-----
----- Cluster
          node_A_1_FC_clus1
          up/up      169.254.209.69/16  node_A_1_FC  e0a
true
          node_A_1_FC_clus2
          up/up      169.254.49.125/16  node_A_1_FC  e0b
true
          node_A_2_FC_clus1
          up/up      169.254.47.194/16  node_A_2_FC  e0a
true
          node_A_2_FC_clus2
          up/up      169.254.19.183/16  node_A_2_FC  e0b
true

4 entries were displayed.

Cluster-A::*>

```

6. Repeat all the previous steps on switch_A_2_IP.
7. Reconnect the local cluster ISL ports.
8. Repeat the above steps at site_B for switch B_1_IP and switch B_2_IP.
9. Connect the remote ISLs between the sites.

Step 2: Verify that the cluster connections are moved and the cluster is healthy

To ensure that there is proper connectivity and that the configuration is ready to proceed with the transition process, verify that the cluster connections are moved correctly, the cluster switches are recognized and the cluster is healthy.

Steps

1. Verify that all cluster ports are up and running:

```
network port show -ipspace Cluster
```

```
Cluster-A::*> network port show -ipspace Cluster
```

Node: Node-A-1-FC

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps)	Health
					Admin/Oper	Status
e0a	Cluster	Cluster	up	9000	auto/10000	healthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy

Node: Node-A-2-FC

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps)	Health
					Admin/Oper	Status
e0a	Cluster	Cluster	up	9000	auto/10000	healthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy

4 entries were displayed.

```
Cluster-A::*>
```

2. Verify that all interfaces are on their home port:

```
network interface show -vserver Cluster
```

This might take several minutes to complete.

The following example shows that all interfaces show true in the “Is Home” column.

```

Cluster-A::*> network interface show -vserver Cluster

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

-----
----- Cluster
      Node-A-1_FC_clus1
      up/up      169.254.209.69/16  Node-A-1_FC  e0a
true
      Node-A-1-FC_clus2
      up/up      169.254.49.125/16  Node-A-1-FC  e0b
true
      Node-A-2-FC_clus1
      up/up      169.254.47.194/16  Node-A-2-FC  e0a
true
      Node-A-2-FC_clus2
      up/up      169.254.19.183/16  Node-A-2-FC  e0b
true

4 entries were displayed.

Cluster-A::*>

```

3. Verify that both the local IP switches are discovered by the nodes:

```
network device-discovery show -protocol cdp
```

```
Cluster-A::*> network device-discovery show -protocol cdp

Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface      Platform
-----  -----  -----
-----  -----
Node-A-1-FC
    /cdp
    e0a    Switch-A-3-IP      1/5/1      N3K-
C3232C
    e0b    Switch-A-4-IP      0/5/1      N3K-
C3232C
Node-A-2-FC
    /cdp
    e0a    Switch-A-3-IP      1/6/1      N3K-
C3232C
    e0b    Switch-A-4-IP      0/6/1      N3K-
C3232C

4 entries were displayed.

Cluster-A::*>
```

4. On the IP switch, verify that the MetroCluster IP nodes have been discovered by both local IP switches:

```
show cdp neighbors
```

You must perform this step on each switch.

This example shows how to verify the nodes are discovered on Switch-A-3-IP.

```
(Switch-A-3-IP) # show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID ID	Local Intrfce	Hldtme	Capability	Platform	Port
Node-A-1-FC	Eth1/5/1	133	H	FAS8200	e0a
Node-A-2-FC	Eth1/6/1	133	H	FAS8200	e0a
Switch-A-4-IP (FDO220329A4)					
	Eth1/7	175	R S I s	N3K-C3232C	Eth1/7
Switch-A-4-IP (FDO220329A4)					
	Eth1/8	175	R S I s	N3K-C3232C	Eth1/8
Switch-B-3-IP (FDO220329B3)					
	Eth1/20	173	R S I s	N3K-C3232C	
Eth1/20					
Switch-B-3-IP (FDO220329B3)					
	Eth1/21	173	R S I s	N3K-C3232C	
Eth1/21					

Total entries displayed: 4

```
(Switch-A-3-IP) #
```

This example shows how to verify that the nodes are discovered on Switch-A-4-IP.

```
(Switch-A-4-IP) # show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC        Eth1/5/1    133      H            FAS8200      e0b
Node-A-2-FC        Eth1/6/1    133      H            FAS8200      e0b
Switch-A-3-IP (FDO220329A3)
                  Eth1/7      175      R S I s      N3K-C3232C  Eth1/7
Switch-A-3-IP (FDO220329A3)
                  Eth1/8      175      R S I s      N3K-C3232C  Eth1/8
Switch-B-4-IP (FDO220329B4)
                  Eth1/20     169      R S I s      N3K-C3232C
Eth1/20
Switch-B-4-IP (FDO220329B4)
                  Eth1/21     169      R S I s      N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-4-IP) #
```

Preparing the MetroCluster IP controllers

You must prepare the four new MetroCluster IP nodes and install the correct ONTAP version.

This task must be performed on each of the new nodes:

- node_A_1-IP
- node_A_2-IP
- node_B_1-IP
- node_B_2-IP

In these steps, you clear the configuration on the nodes and clear the mailbox region on new drives.

1. Rack the new controllers for the MetroCluster IP configuration.

The MetroCluster FC nodes (node_A_x-FC and node_B_x-FC) remain cabled at this time.

2. Cable the MetroCluster IP nodes to the IP switches as shown in the [Cabling the IP switches](#).
3. Configure the MetroCluster IP nodes using the following sections:

- a. Gather required information
- b. Restore system defaults on a controller module
- c. Verify the ha-config state of components
- d. Manually assign 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.

5. Repeat these steps on the other MetroCluster IP nodes.

Configure the MetroCluster for transition

To prepare the configuration for transition you add the new nodes to the existing MetroCluster configuration and then move data to the new nodes.

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:

```
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
```

2. Repeat the command on the partner cluster.

Enabling transition mode and disabling cluster HA

You must enable the MetroCluster transition mode to allow the old and new nodes to operate together in the MetroCluster configuration, and disable cluster HA.

1. Enable transition:
 - a. Change to the advanced privilege level:

```
set -privilege advanced
```

- b. Enable transition mode:

```
metrocluster transition enable -transition-mode non-disruptive
```



Run this command on one cluster only.

```
cluster_A::*> metrocluster transition enable -transition-mode non-disruptive
```

Warning: This command enables the start of a "non-disruptive" MetroCluster

FC-to-IP transition. It allows the addition of hardware for another DR

group that uses IP fabrics, and the removal of a DR group that uses FC

fabrics. Clients will continue to access their data during a non-disruptive transition.

Automatic unplanned switchover will also be disabled by this command.

Do you want to continue? {y|n}: y

```
cluster_A::*>
```

c. Return to the admin privilege level:

```
set -privilege admin
```

2. Verify that transition is enabled on both the clusters.

```
cluster_A::> metrocluster transition show-mode  
Transition Mode
```

non-disruptive

```
cluster_A::*>
```

```
cluster_B::*> metrocluster transition show-mode  
Transition Mode
```

non-disruptive

```
Cluster_B::>
```

3. Disable cluster HA.



You must run this command on both clusters.

```
cluster_A::*> cluster ha modify -configured false
```

Warning: This operation will unconfigure cluster HA. Cluster HA must be configured on a two-node cluster to ensure data access availability in the event of storage failover.

Do you want to continue? {y|n}: y

Notice: HA is disabled.

```
cluster_A::*>
```

```
cluster_B::*> cluster ha modify -configured false
```

Warning: This operation will unconfigure cluster HA. Cluster HA must be configured on a two-node cluster to ensure data access availability in the event of storage failover.

Do you want to continue? {y|n}: y

Notice: HA is disabled.

```
cluster_B::*>
```

4. Verify that cluster HA is disabled.



You must run this command on both clusters.

```

cluster_A::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_A::>

cluster_B::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_B::>

```

Joining the MetroCluster IP 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 MetroCluster IP nodes to the existing MetroCluster configuration.
 - a. Join the first MetroCluster IP node (node_A_3-IP) to the existing MetroCluster FC 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]:
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 MetroCluster IP node (node_A_4-IP) to the existing MetroCluster FC configuration.
2. Repeat these steps to join node_B_3-IP and node_B_4-IP to cluster_B.

3. If you are using the Onboard Key Manager, perform the following steps from the cluster where you've added a new node:

- Synchronize the key manager configuration:

```
security key-manager onboard sync
```

- Enter the Onboard Key Manager passphrase when prompted.

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

- On the new MetroCluster IP nodes, [configure the intercluster LIFs](#).
- 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
```

3. Configure the DR group for the MetroCluster IP nodes:

```
metrocluster configuration-settings dr-group create -partner-cluster
```

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_3-IP -remote-node node_B_3-IP
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Verify that the DR group is created.

```
metrocluster configuration-settings dr-group show
```

```
cluster_A::> metrocluster configuration-settings dr-group show
```

DR Group ID	Cluster Node	Node	DR Partner
2	cluster_A	node_A_3-IP node_A_4-IP	node_B_3-IP node_B_4-IP
	cluster_B	node_B_3-IP node_B_4-IP	node_A_3-IP node_A_4-IP

4 entries were displayed.

```
cluster_A::>
```

You will notice that the DR group for the old MetroCluster FC nodes (DR Group 1) is not listed when you run the `metrocluster configuration-settings dr-group show` command.

You can use `metrocluster node show` command on both sites to list all nodes.

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

DR	Configuration	DR			
Group	Cluster	Node	State	Mirroring	Mode
1	cluster_A				
		node_A_1-FC	configured	enabled	normal
		node_A_2-FC	configured	enabled	normal
	cluster_B				
		node_B_1-FC	configured	enabled	normal
		node_B_2-FC	configured	enabled	normal
2	cluster_A				
		node_A_3-IP	ready to configure	-	-
		node_A_4-IP	ready to configure	-	-

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

DR	Configuration	DR			
Group	Cluster	Node	State	Mirroring	Mode
1	cluster_B				
		node_B_1-FC	configured	enabled	normal
		node_B_2-FC	configured	enabled	normal
	cluster_A				
		node_A_1-FC	configured	enabled	normal
		node_A_2-FC	configured	enabled	normal
2	cluster_B				
		node_B_3-IP	ready to configure	-	-
		node_B_4-IP	ready to configure	-	-

5. Configure the MetroCluster IP interfaces for the newly joined MetroCluster IP nodes:



Do not use 169.254.17.x or 169.254.18.x IP addresses when you create MetroCluster IP interfaces to avoid conflicts with system auto-generated interface IP addresses in the same range.

```
metrocluster configuration-settings interface create -cluster-name
```

See [Configuring and connecting the MetroCluster IP interfaces](#) for considerations when configuring the IP interfaces.



You can configure the MetroCluster IP interfaces from either cluster.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port ela -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_3-IP -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_4-IP -home-port ela -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_4-IP -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_3-IP -home-port ela -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_3-IP -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_4-IP -home-port ela -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_4-IP -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
-----
-----
2      cluster_A
      node_A_3-IP
          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_4-IP
          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_3-IP
          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_3-IP
          Home Port: e1a
          172.17.26.12    255.255.255.0    -
completed
          Home Port: e1b
          172.17.27.12    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

-----
-----
```

2	cluster_A	node_A_3-IP**				
		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_4-IP				
		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: e1b		
		172.17.27.11	172.17.27.10	HA Partner
completed		Home Port: e1b		
		172.17.27.11	172.17.27.13	DR Partner
completed		Home Port: e1b		
		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_4-IP			
	Home Port: e1a			
	172.17.26.13	172.17.26.12	HA Partner	
completed	Home Port: e1a			
	172.17.26.13	172.17.26.11	DR Partner	
completed	Home Port: e1a			
	172.17.26.13	172.17.26.10	DR Auxiliary	
completed	Home Port: e1b			
	172.17.27.13	172.17.27.12	HA Partner	
completed	Home Port: e1b			
	172.17.27.13	172.17.27.11	DR Partner	
completed	Home Port: e1b			
	172.17.27.13	172.17.27.10	DR Auxiliary	
completed				
	node_B_3-IP			
	Home Port: e1a			
	172.17.26.12	172.17.26.13	HA Partner	
completed	Home Port: e1a			
	172.17.26.12	172.17.26.10	DR Partner	
completed	Home Port: e1a			
	172.17.26.12	172.17.26.11	DR Auxiliary	

```
completed
      Home Port: e1b
      172.17.27.12    172.17.27.13    HA Partner
completed
      Home Port: e1b
      172.17.27.12    172.17.27.10    DR Partner
completed
      Home Port: e1b
      172.17.27.12    172.17.27.11    DR Auxiliary
completed
24 entries were displayed.

cluster_A::>
```

9. Verify disk autoassignment and partitioning:

```
disk show -pool Pool1
```

```

cluster_A::> disk show -pool Pool1
      Usable          Disk      Container      Container
Disk      Size Shelf Bay Type      Type      Name
Owner

-----
1.10.4          -   10   4 SAS      remote      -
node_B_2
1.10.13         -   10  13 SAS      remote      -
node_B_2
1.10.14         -   10  14 SAS      remote      -
node_B_1
1.10.15         -   10  15 SAS      remote      -
node_B_1
1.10.16         -   10  16 SAS      remote      -
node_B_1
1.10.18         -   10  18 SAS      remote      -
node_B_2
...
2.20.0          546.9GB  20   0 SAS      aggregate  aggr0_rhal_a1
node_a_1
2.20.3          546.9GB  20   3 SAS      aggregate  aggr0_rhal_a2
node_a_2
2.20.5          546.9GB  20   5 SAS      aggregate  rhal_a1_aggr1
node_a_1
2.20.6          546.9GB  20   6 SAS      aggregate  rhal_a1_aggr1
node_a_1
2.20.7          546.9GB  20   7 SAS      aggregate  rhal_a2_aggr1
node_a_2
2.20.10         546.9GB  20  10 SAS      aggregate  rhal_a1_aggr1
node_a_1
...
43 entries were displayed.
cluster_A::>

```



On systems configured for Advanced Drive Partitioning (ADP), the container type is "shared" rather than "remote" as shown in the example output.

10. Mirror the root aggregates:

```
storage aggregate mirror -aggregate aggr0_node_A_3_IP
```



You must complete this step on each MetroCluster IP node.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_3_IP

Info: Disks would be added to aggregate "aggr0_node_A_3_IP" on node
"node_A_3-IP"
in the following manner:
```

Second Plex

RAID Group rg0, 3 disks (block checksum, raid_dp)

Physical Size	Position	Disk	Type	Usable Size
-----	-----	-----	-----	-----
-	dparity	4.20.0	SAS	-
-	parity	4.20.3	SAS	-
-	data	4.20.1	SAS	546.9GB
558.9GB				

Aggregate capacity available for volume 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_FC
      349.0GB    16.84GB    95% online      1  node_A_1-FC
raid_dp,
mirrored,
normal
```

```

aggr0_node_A_2_FC
    349.0GB    16.84GB    95% online      1 node_A_2-FC
    raid_dp,
    mirrored,
    normal
    aggr0_node_A_3_IP
        467.6GB    22.63GB    95% online      1 node_A_3-IP
    raid_dp,
    mirrored,
    normal
    aggr0_node_A_4_IP
        467.6GB    22.62GB    95% online      1 node_A_4-IP
    raid_dp,
    mirrored,
    normal
    aggr_data_a1
        1.02TB    1.01TB    1% online      1 node_A_1-FC
    raid_dp,
    mirrored,
    normal
    aggr_data_a2
        1.02TB    1.01TB    1% online      1 node_A_2-FC
    raid_dp,
    mirrored,

```

Finalizing the addition of the MetroCluster IP nodes

You must incorporate the new DR group into the MetroCluster configuration and create mirrored data aggregates on the new nodes.

Steps

1. Configure the MetroCluster depending on whether there is a single or multiple data aggregates on both clusters:

If your MetroCluster configuration has...	Then do this...
---	-----------------

Multiple data aggregates on both clusters	<p>From any node's prompt, configure MetroCluster:</p> <pre>metrocluster configure <node-name></pre> <p> You must run <code>metrocluster configure</code> and not <code>metrocluster configure -refresh true</code></p>
A single mirrored data aggregate on both clusters	<p>a. From any node's prompt, change to the advanced privilege level:</p> <pre>set -privilege advanced</pre> <p>You must respond with <code>y</code> when you are prompted to continue into advanced mode and you see the advanced mode prompt (<code>*></code>).</p> <p>b. Configure the MetroCluster with the <code>-allow-with-one-aggregate true</code> parameter:</p> <pre>metrocluster configure -allow-with-one-aggregate true -node-name <node-name></pre> <p>c. Return to the admin privilege level:</p> <pre>set -privilege admin</pre>



The best practice is to have multiple mirrored data aggregates. When there is only one mirrored aggregate, there is less protection because the metadata volumes are located on the same aggregate rather than on separate aggregates.

2. Reboot each of the new nodes:

```
node reboot -node <node_name> -inhibit-takeover true
```



You don't need to reboot the nodes in a specific order, but you should wait until one node is fully booted and all connections are established before rebooting the next node.

3. Verify that the nodes are added to their DR group:

```
metrocluster node show
```

4. 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 acceptable 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_3-IP.

```

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::>
```

5. Verify that all nodes in the cluster are healthy:

```
cluster show
```

The output should display `true` for the `health` field for all nodes.

6. Confirm that takeover is possible and the nodes are connected by running the following command on both clusters:

```
storage failover show
```

cluster_A::> storage failover show		Takeover Possible	State Description
Node	Partner		
Node_FC_1	Node_FC_2	true	Connected to Node_FC_2
Node_FC_2	Node_FC_1	true	Connected to Node_FC_1
Node_IP_1	Node_IP_2	true	Connected to Node_IP_2
Node_IP_2	Node_IP_1	true	Connected to Node_IP_1

7. Confirm that all disks attached to the newly-joined MetroCluster IP nodes are present:

```
disk show
```

8. Verify the health of the MetroCluster configuration by running the following commands:

- metrocluster check run
- metrocluster check show
- metrocluster interconnect mirror show
- metrocluster interconnect adapter show

9. Move the MDV_CRS volumes from the old nodes to the new nodes in advanced privilege.

- 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.
```

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
```

Moving the data to the new drive shelves

During the transition, you move data from the drive shelves in the MetroCluster FC configuration to the new MetroCluster IP configuration.

Before you begin

You should create new SAN LIFs on the destination or IP nodes and connect hosts prior to moving volumes to new the new aggregates.

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.

2. Move the data volumes to aggregates on the new controllers, one volume at a time.

Use the procedure in [Creating an aggregate and moving volumes to the new nodes](#).

3. Create SAN LIFs on the recently added nodes.

Use the following procedure in [Updating LUN paths for the new nodes](#).

4. Check if there are any node locked licenses on the FC nodes, if there are, they need to be added to the newly added nodes.

Use the following procedure in [Adding node-locked licenses](#).

5. Migrate the data LIFs.

Use the procedure in [Moving non-SAN data LIFs and cluster management LIFs to the new nodes](#) but do **not** perform the last two steps to migrate cluster management LIFs.

 • You cannot migrate a LIF that is used for copy-offload operations with VMware vStorage APIs for Array Integration (VAAI).

• After you complete the transition of your MetroCluster nodes from FC to IP, you might need to move your iSCSI host connections to the new nodes, see [Moving Linux iSCSI hosts from MetroCluster FC to MetroCluster IP nodes](#).

Removing the MetroCluster FC controllers

You must perform clean-up tasks and remove the old controller modules from the MetroCluster configuration.

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.
2. Identify the aggregates hosted on the MetroCluster FC configuration that need to be deleted.

In this example the following data aggregates are hosted by the MetroCluster FC cluster_B and need to be deleted: `aggr_data_a1` and `aggr_data_a2`.



You need to perform the steps to identify, offline and delete the data aggregates on both the clusters. The example is for one cluster only.


```

mirrored,
normal
aggr_data_a3
    1.37TB      1.35TB      1% online      3 node_A_3-IP
raid_dp,
mirrored,
normal
aggr_data_a4
    1.25TB      1.24TB      1% online      2 node_A_4-IP
raid_dp,
mirrored,
normal
8 entries were displayed.

```

cluster_B::>

3. Check if the data aggregates on the FC nodes have any MDV_aud volumes, and delete them prior to deleting the aggregates.

You must delete the MDV_aud volumes as they cannot be moved.

4. Take each of the data aggregates offline, and then delete them:

- a. Take the aggregate offline: storage aggregate offline -aggregate aggregate-name

The following example shows the aggregate aggr_data_a1 being taken offline:

```

cluster_B::> storage aggregate offline -aggregate aggr_data_a1
Aggregate offline successful on aggregate: aggr_data_a1

```

- b. Delete the aggregate: storage aggregate delete -aggregate aggregate-name

You can destroy the plex when prompted.

The following example shows the aggregate aggr_data_a1 being deleted.

```

cluster_B::> storage aggregate delete -aggregate aggr_data_a1
Warning: Are you sure you want to destroy aggregate "aggr_data_a1"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>

```

5. Identify the MetroCluster FC DR group that need to be removed.

In the following example the MetroCluster FC nodes are in DR Group '1', and this is the DR group that need to be removed.

```

cluster_B::> metrocluster node show

DR                                         Configuration  DR
Group Cluster Node          State          Mirroring Mode
-----  -----  -----  -----  -----
-----  -----
1      cluster_A
        node_A_1-FC      configured  enabled   normal
        node_A_2-FC      configured  enabled   normal
      cluster_B
        node_B_1-FC      configured  enabled   normal
        node_B_2-FC      configured  enabled   normal
2      cluster_A
        node_A_3-IP      configured  enabled   normal
        node_A_4-IP      configured  enabled   normal
      cluster_B
        node_B_3-IP      configured  enabled   normal
        node_B_3-IP      configured  enabled   normal
8 entries were displayed.

cluster_B::>

```

6. Move the cluster management LIF from a MetroCluster FC node to a MetroCluster IP node:

```
cluster_B::> network interface migrate -vserver svm-name -lif cluster_mgmt
-destination-node node-in-metrocluster-ip-dr-group -destination-port
available-port
```

7. Change the home node and home port of the cluster management LIF: `cluster_B::> network interface modify -vserver svm-name -lif cluster_mgmt -service-policy default-management -home-node node-in-metrocluster-ip-dr-group -home-port lif-port`

8. Move epsilon from a MetroCluster FC node to a MetroCluster IP node:

a. Identify which node currently has epsilon: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node          epsilon
-----
node_A_1-FC    true
node_A_2-FC    false
node_A_1-IP    false
node_A_2-IP    false
4 entries were displayed.
```

- b. Set epsilon to false on the MetroCluster FC node (node_A_1-FC): `cluster modify -node fc-node -epsilon false`
- c. Set epsilon to true on the MetroCluster IP node (node_A_1-IP): `cluster modify -node ip-node -epsilon true`
- d. Verify that epsilon has moved to the correct node: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node          epsilon
-----
node_A_1-FC    false
node_A_2-FC    false
node_A_1-IP    true
node_A_2-IP    false
4 entries were displayed.
```

- 9. Modify the IP address for the cluster peer of the transitioned IP nodes for each cluster:

- a. Identify the cluster_A peer by using the `cluster peer show` command:

```
cluster_A::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication

-----
cluster_B          1-80-000011          Unavailable      absent
```

- i. Modify the cluster_A peer IP address:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

- b. Identify the cluster_B peer by using the `cluster peer show` command:

```

cluster_B::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication

-----
-----
cluster_A          1-80-000011      Unavailable      absent

```

i. Modify the cluster_B peer IP address:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

c. Verify that the cluster peer IP address is updated for each cluster:

i. Verify that the IP address is updated for each cluster by using the `cluster peer show -instance` command.

The `Remote Intercluster Addresses` field in the following examples displays the updated IP address.

Example for cluster_A:

```

cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
                    Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
                    Availability of the Remote Cluster: Available
                    Remote Cluster Name: cluster_B
                    Active IP Addresses: 172.21.178.212,
172.21.178.204
                    Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
node_B_4-IP
                    Remote Cluster Health: true
                    Unreachable Local Nodes: -
                    Address Family of Relationship: ipv4
                    Authentication Status Administrative: use-authentication
                    Authentication Status Operational: ok
                    Last Update Time: 4/20/2023 18:23:53
                    IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
Algorithm By Which the PSK Was Derived: jpake

cluster_A::>

```

Example for cluster_B

```
cluster_B::> cluster peer show -instance

          Peer Cluster Name: cluster_A
          Remote Intercluster Addresses: 172.21.178.188,
172.21.178.196 <<<<<< Should reflect the modified address
          Availability of the Remote Cluster: Available
          Remote Cluster Name: cluster_A
          Active IP Addresses: 172.21.178.196,
172.21.178.188
          Cluster Serial Number: 1-80-000011
          Remote Cluster Nodes: node_A_3-IP,
                               node_A_4-IP
          Remote Cluster Health: true
          Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
          Authentication Status Administrative: use-authentication
          Authentication Status Operational: ok
          Last Update Time: 4/20/2023 18:23:53
          IPspace for the Relationship: Default
          Proposed Setting for Encryption of Inter-Cluster Communication: -
          Encryption Protocol For Inter-Cluster Communication: tls-psk
          Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. On each cluster, remove the DR group containing the old nodes from the MetroCluster FC configuration.

You must perform this step on both clusters, one at a time.

```
cluster_B::> metrocluster remove-dr-group -dr-group-id 1

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_B::>
```

11. Verify that the nodes are ready to be removed from the clusters.

You must perform this step on both clusters.



At this point, the metrocluster node show command only shows the local MetroCluster FC nodes and no longer shows the nodes that are part of the partner cluster.

```

cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node             State        Mirroring Mode
-----  -----  -----  -----
-----  -----
1      cluster_A
      node_A_1-FC      ready to configure      -      -
      node_A_2-FC      ready to configure      -      -
2      cluster_A
      node_A_3-IP      configured      enabled      normal
      node_A_4-IP      configured      enabled      normal
      cluster_B
      node_B_3-IP      configured      enabled      normal
      node_B_4-IP      configured      enabled      normal
6 entries were displayed.

cluster_B::>

```

12. Disable storage failover for the MetroCluster FC nodes.

You must perform this step on each node.

```

cluster_A::> storage failover modify -node node_A_1-FC -enabled false
cluster_A::> storage failover modify -node node_A_2-FC -enabled false
cluster_A::>

```

13. Unjoin the MetroCluster FC nodes from the clusters: `cluster unjoin -node node-name`

You must perform this step on each node.

```
cluster_A::> cluster unjoin -node node_A_1-FC

Warning: This command will remove node "node_A_1-FC" from the cluster.
You must
        remove the failover partner as well. After the node is removed,
erase
        its configuration and initialize all disks by using the "Clean
        configuration and initialize all disks (4)" option from the
boot menu.

Do you want to continue? {y|n}: y
[Job 553] Job is queued: Cluster remove-node of Node:node_A_1-FC with
UUID:6c87de7e-ff54-11e9-8371
[Job 553] Checking prerequisites
[Job 553] Cleaning cluster database
[Job 553] Job succeeded: Node remove succeeded
If applicable, also remove the node's HA partner, and then clean its
configuration and initialize all disks with the boot menu.
Run "debug vreport show" to address remaining aggregate or volume
issues.

cluster_B::>
```

14. If the configuration uses FC-to-SAS bridges or FC back-end switches, disconnect and remove them.

Remove FC-to-SAS bridges

- Identify the bridges:

```
system bridge show
```

- Remove the bridges:

```
system bridge remove -name <bridge_name>
```

- Confirm the bridges are removed:

```
system bridge show
```

The following example shows that the bridges are removed:

Example

```
cluster1::> system bridge remove -name ATTO_10.226.197.16
cluster1::> system bridge show

Is      Monitor
Bridge   Symbolic Name Vendor  Model      Bridge WWN
Monitored Status
-----
-----
ATTO_FibreBridge6500N_1
      Bridge Number 16
                  Atto      FibreBridge 6500N
                                2000001086603824
false   -
ATTO_FibreBridge6500N_2
      Not Set        Atto      FibreBridge 6500N
                                20000010866037e8
false   -
ATTO_FibreBridge6500N_3
      Not Set        Atto      FibreBridge 6500N
                                2000001086609e0e
false   -
ATTO_FibreBridge6500N_4
      Not Set        Atto      FibreBridge 6500N
                                2000001086609c06
false   -
4 entries were displayed.
```

Remove FC switches

a. Identify the switches:

```
system switch fibre-channel show
```

b. Remove the switches:

```
system switch fibre-channel remove -switch-name <switch_name>
```

c. Confirm the switches are removed:

```
system switch fibre-channel show
```

Example

```
cluster1::> system switch fibre-channel show
                           Symbolic                         Is
Monitor
  Switch      Name      Vendor  Model      Switch WWN
Monitored Status
-----
-----
Cisco_10.226.197.34
  mcc-cisco-8Gb-fab-4
    Cisco    DS-C9148-16P-K9
                                         2000547fee78f088
  true      ok
  mcc-cisco-8Gb-fab-1
    mcc-cisco-8Gb-fab-1
      Cisco    -
  false      -
  mcc-cisco-8Gb-fab-2
    mcc-cisco-8Gb-fab-2
      Cisco    -
  false      -
  mcc-cisco-8Gb-fab-3
    mcc-cisco-8Gb-fab-3
      Cisco    -
  false      -
  4 entries were displayed.

cluster1::> system switch fibre-channel remove -switch-name
Cisco_10.226.197.34
cluster1::> system switch fibre-channel show
                           Symbolic                         Is
Monitor
  Switch      Name      Vendor  Model      Switch WWN
Monitored Status
-----
-----
  mcc-cisco-8Gb-fab-4
    mcc-cisco-8Gb-fab-4
      Cisco
      -
  false      -
  mcc-cisco-8Gb-fab-1
    mcc-cisco-8Gb-fab-1
      Cisco    -
  false      -
  mcc-cisco-8Gb-fab-2
```

```

mcc-cisco-8Gb-fab-2
Cisco      -
false      -
mcc-cisco-8Gb-fab-3
Cisco      -
false      -
4 entries were displayed
cluster1::>

```

15. Power down the MetroCluster FC controller modules and storage shelves.
16. Disconnect and remove the MetroCluster FC controller modules and storage shelves.

Completing the transition

To complete the transition you must verify the operation of the new MetroCluster IP configuration.

1. Verify the MetroCluster IP configuration.

You must perform this step on each cluster in advanced privilege mode.

The following example shows the output for cluster_A.

```

cluster_A::> cluster show
Node          Health  Eligibility  Epsilon
-----  -----
node_A_1-IP    true    true        false
node_A_2-IP    true    true        false
2 entries were displayed.

cluster_A::>

```

The following example shows the output for cluster_B.

```

cluster_B::> cluster show
Node          Health  Eligibility  Epsilon
-----  -----
node_B_1-IP    true    true        false
node_B_2-IP    true    true        false
2 entries were displayed.

cluster_B::>

```

2. Enable cluster HA and storage failover.

You must perform this step on each cluster.

3. Verify that cluster HA capability is enabled.

```
cluster_A::> cluster ha show
High Availability Configured: true

cluster_A::>

cluster_A::> storage failover show
                           Takeover
  Node          Partner      Possible State Description
  -----  -----  -----
  -----
  node_A_1-IP    node_A_2-IP    true      Connected to node_A_2-IP
  node_A_2-IP    node_A_1-IP    true      Connected to node_A_1-IP
2 entries were displayed.

cluster_A::>
```

4. Disable MetroCluster transition mode.

- Change to the advanced privilege level: `set -privilege advanced`
- Disable transition mode: `metrocluster transition disable`
- Return to the admin privilege level: `set -privilege admin`

```
cluster_A::*> metrocluster transition disable

cluster_A::*>
```

5. Verify that transition is disabled: `metrocluster transition show-mode`

You must perform these steps on both clusters.

```
cluster_A::> metrocluster transition show-mode
Transition Mode
-----
not-enabled

cluster_A::>
```

```

cluster_B::> metrocluster transition show-mode
Transition Mode
-----
not-enabled

cluster_B::>

```

6. If you have an eight-node configuration, you must repeat the entire procedure starting from [Prepare for transition from a MetroCluster FC to a MetroCluster IP configuration](#) for each of the FC DR groups.

Sending a custom AutoSupport message after maintenance

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

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 or Mediator monitoring

After completing the transition of the MetroCluster configuration, you can resume monitoring with the Tiebreaker or Mediator utility.

1. Use the appropriate procedure for your configuration.

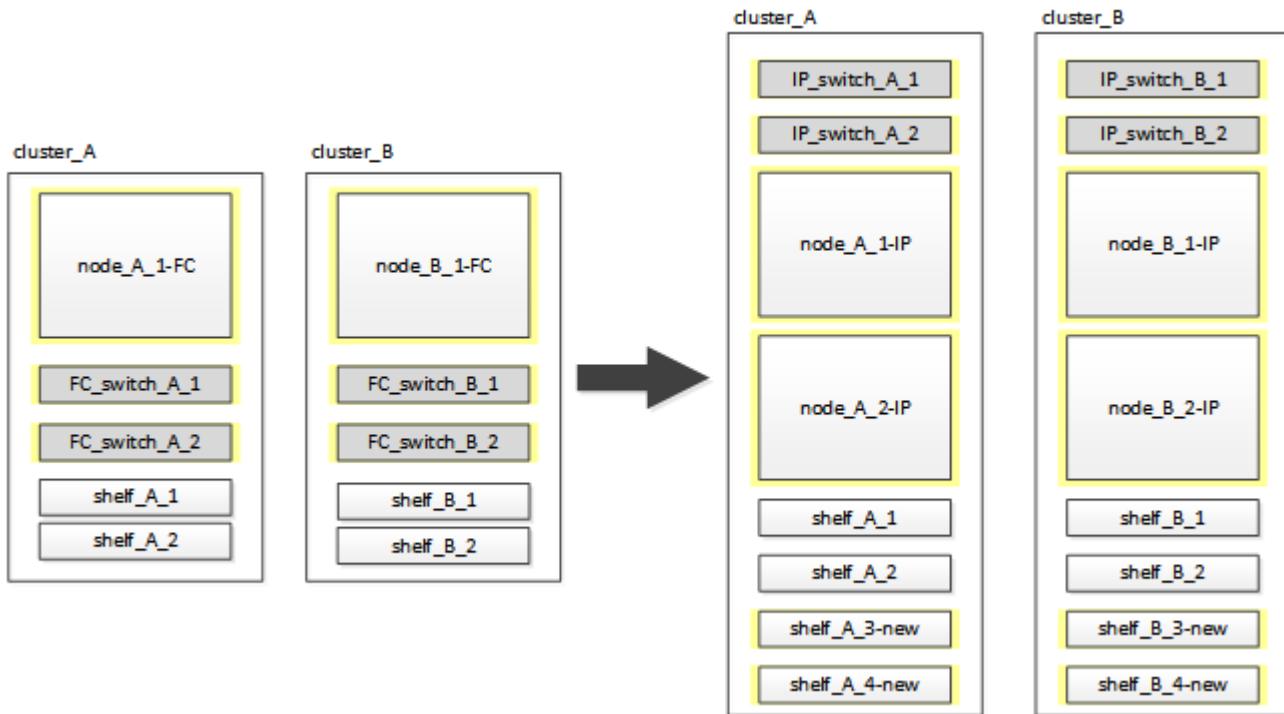
If you are using...	Use this procedure
Tiebreaker	Adding MetroCluster configurations
Mediator	Configure ONTAP Mediator from a MetroCluster IP configuration

Disruptively transition from a two-node MetroCluster FC to a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Disruptively transitioning from a two-node MetroCluster FC to a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Beginning with ONTAP 9.8, you can transition workloads and data from an existing two-node MetroCluster FC configuration to a new four-node MetroCluster IP configuration. Disk shelves from the MetroCluster FC nodes are moved to the IP nodes.

The following illustration provides a simplified view of the configuration before and after this transition procedure.



- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is disruptive.
- This procedure applies only to a two-node MetroCluster FC configuration.

If you have a four-node MetroCluster FC configuration, see [Choosing your transition procedure](#).

- ADP is not supported on the four-node MetroCluster IP configuration created by this procedure.
- You must meet all requirements and follow all steps in the procedure.
- The existing storage shelves are moved to the new MetroCluster IP nodes.
- Additional storage shelves can be added to the configuration if necessary.

See [Drive shelf reuse and drive requirements for disruptive FC-to-IP transition](#).

Example naming in this procedure

This procedure uses example names throughout to identify the DR groups, nodes, and switches involved.

The nodes in the original configuration have the suffix -FC, indicating that they are in a fabric-attached or stretch MetroCluster configuration.

Components	cluster_A at site_A	cluster_B at site_B
------------	---------------------	---------------------

dr_group_1-FC	<ul style="list-style-type: none"> node_A_1-FC shelf_A_1 shelf_A_2 	<ul style="list-style-type: none"> node_B_1-FC shelf_B_1 shelf_B_2
dr_group_2-IP	<ul style="list-style-type: none"> node_A_1-IP node_A_2-IP shelf_A_1 shelf_A_2 shelf_A_3-new shelf_A_4-new 	<ul style="list-style-type: none"> node_B_1-IP node_B_2-IP shelf_B_1 shelf_B_2 shelf_B_3-new shelf_B_4-new
Switches	<ul style="list-style-type: none"> switch_A_1-FC switch_A_2-FC switch_A_1-IP switch_A_2-IP 	<ul style="list-style-type: none"> switch_B_1-FC switch_B_2-FC switch_B_1-IP switch_B_2-IP

Preparing for disruptive FC-to-IP transition

Before starting the transition process, you must make sure the configuration meets the requirements.

Enable console logging

NetApp strongly recommends that you enable console logging on the devices that you are using and take the following actions when performing this procedure:

- Leave AutoSupport enabled during maintenance.
- Trigger a maintenance AutoSupport message before and after maintenance to disable case creation for the duration of the maintenance activity.

See the Knowledge Base article [How to suppress automatic case creation during scheduled maintenance windows](#).

- Enable session logging for any CLI session. For instructions on how to enable session logging, review the "Logging Session Output" section in the Knowledge Base article [How to configure PuTTY for optimal connectivity to ONTAP systems](#).

General requirements for disruptive FC-to-IP transition

The existing MetroCluster FC configuration must meet the following requirements:

- It must be a two-node configuration and all nodes must be running ONTAP 9.8 or later.

It can be a two-node fabric-attached or stretched MetroCluster.

- It must meet all requirements and cabling as described in the *MetroCluster Installation and Configuration* procedures.

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

[Stretch MetroCluster installation and configuration](#)

- It cannot be configured with NetApp Storage Encryption (NSE).
- The MDV volumes cannot be encrypted.

You must have remote console access for all six nodes from either MetroCluster site or plan for travel between the sites as required by the procedure.

Drive shelf reuse and drive requirements for disruptive FC-to-IP transition

You must ensure that adequate spare drives and root aggregate space is available on the storage shelves.

Reusing the existing storage shelves

When using this procedure, the existing storage shelves are retained for use by the new configuration. When node_A_1-FC and node_B_1-FC are removed, the existing drive shelves are connected to node_A_1-IP and node_A_2-IP on cluster_A and to node_B_1-IP and node_B_2-IP on cluster_B.

- The existing storage shelves (those attached to node_A_1-FC and node_B_1-FC) must be supported by the new platform models.

If the existing shelves are not supported by the new platform models, see [Disruptively transitioning when existing shelves are not supported on new controllers \(ONTAP 9.8 and later\)](#).

- You must ensure you don't exceed the platform limits for drives, etc.

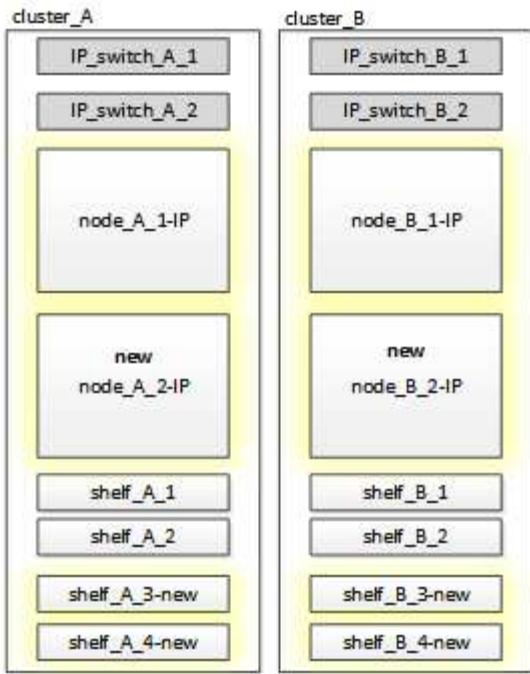
[NetApp Hardware Universe](#)

Storage requirements for the additional controllers

Additional storage must be added, if necessary, to accommodate the two additional controllers (node_A_2-IP and node_B_2-ip), because the configuration is changing from a two-node to a four-node arrangement.

- Depending on the spare drives available in the existing shelves, additional drives must be added to accommodate the additional controllers in the configuration.

This might require additional storage shelves, as shown in the following illustration.



You need to have additional 14 - 18 drives each for the third and fourth controllers (node_A_2-IP and node_B_2-IP):

- Three pool0 drives
- Three pool1 drives
- Two spare drives
- Six to ten drives for the system volume
- You must ensure that the configuration, including the new nodes, does not exceed the platform limits for the configuration, including drive count, root aggregate size capacity, etc.

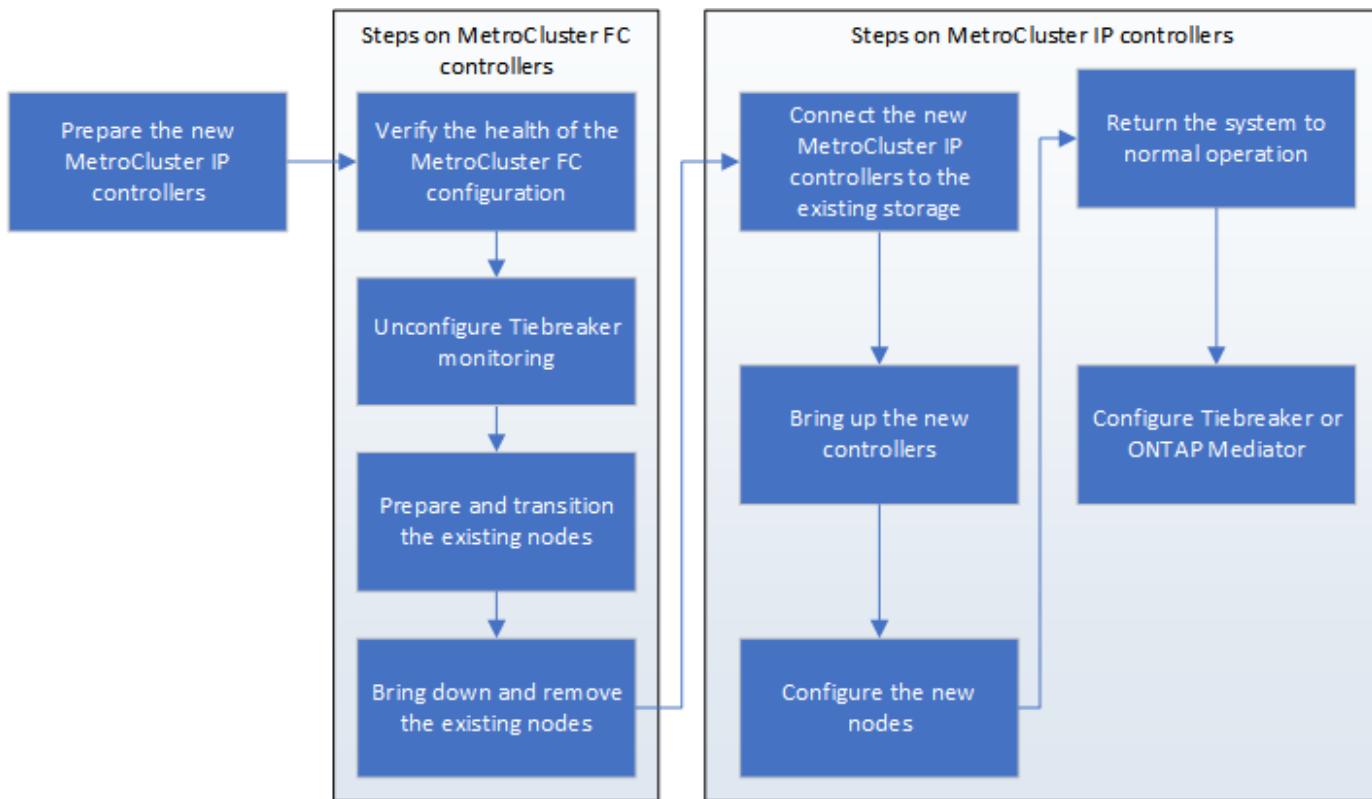
This information is available for each platform model at *NetApp Hardware Universe*.

[NetApp Hardware Universe](#)

Workflow for disruptive transition

You must follow the specific workflow to ensure a successful transition.

As you prepare for the transition, plan for travel between the sites. Note that after the remote nodes are racked and cabled, you need serial terminal access to the nodes. Service Processor access is not available until the nodes are configured.



Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes

You must adjust the port and LIF configuration of the MetroCluster FC node so it is compatible with that of the MetroCluster IP node that will replace it.

About this task

When the new nodes are first booted during the upgrade process, each node uses the most recent configuration of the node it is replacing. When you boot node_A_1-IP, ONTAP attempts to host LIFs on the same ports that were used on node_A_1-FC.

During the transition procedure, you will perform steps on both the old and new nodes to ensure correct cluster, management, and data LIF configuration.

Steps

1. Identify any conflicts between the existing MetroCluster FC port usage and the port usage for the MetroCluster IP interfaces on the new nodes.

You must identify the MetroCluster IP ports on the new MetroCluster IP controllers using the table below. Then check and record if any data LIFs or cluster LIFs exist on those ports on the MetroCluster FC nodes.

These conflicting data LIFs or cluster LIFs on the MetroCluster FC nodes will be moved at the appropriate step in the transition procedure.

The following table shows the MetroCluster IP ports by platform model. You can ignore the VLAN ID column.

Platform model	MetroCluster IP port	VLAN ID	
----------------	----------------------	---------	--

AFF A800	e0b	Not used	
	e1b		
AFF A700 and FAS9000	e5a		
	e5b		
AFF A320	e0g		
	e0h		
AFF A300 and FAS8200	e1a		
	e1b		
FAS8300/A400/FAS8700	e1a	10	
	e1b	20	
AFF A250 and FAS500f	e0c	10	
	e0b	20	

You can fill in the following table and refer to it later in the transition procedure.

Ports	Corresponding MetroCluster IP interface ports (from table above)	Conflicting LIFs on these ports on the MetroCluster FC nodes
First MetroCluster IP port on node_A_1-FC		
Second MetroCluster IP port on node_A_1-FC		
First MetroCluster IP port on node_B_1-FC		
Second MetroCluster IP port on node_B_1-FC		

2. Determine which physical ports are available on the new controllers and which LIFs can be hosted on the ports.

The controller's port usage depends on the platform model and IP switch model you will use in the MetroCluster IP configuration. You can gather the port usage of the new platforms from the *NetApp*

Hardware Universe.

[NetApp Hardware Universe](#)

3. If desired, record the port information for node_A_1-FC and node_A_1-IP.

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

In the columns for node_A_1-IP, add the physical ports for the new controller module and plan the IPspaces and broadcast domains for the new node.

	node_A_1-FC			node_A_1-IP		
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						

4. If desired, record all the port information for node_B_1-FC.

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

In the columns for node_B_1-IP, add the physical ports for the new controller module and plan the LIF port usage, IPspaces and broadcast domains for the new node.

	node_B_1-FC			node_B_1-IP		
LIF	Physical ports	IPspaces	Broadcast domains	Physical 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						

Preparing the MetroCluster IP controllers

You must prepare the four new MetroCluster IP nodes and install the correct ONTAP version.

About this task

This task must be performed on each of the new nodes:

- node_A_1-IP
- node_A_2-IP
- node_B_1-IP
- node_B_2-IP

The nodes should be connected to any **new** storage shelves. They must **not** be connected to the existing storage shelves containing data.

These steps can be performed now, or later in the procedure when the controllers and shelves are racked. In

any case, you must make sure you clear the configuration and prepare the nodes **before** connecting them to the existing storage shelves and **before** making any configuration changes to the MetroCluster FC nodes.



Do not perform these steps with the MetroCluster IP controllers connected to the existing storage shelves that were connected to the MetroCluster FC controllers.

In these steps, you clear the configuration on the nodes and clear the mailbox region on new drives.

Steps

1. Connect the controller modules to the new storage shelves.
2. 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”.

3. 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
```

4. Exit Maintenance mode:

```
halt
```

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

5. Repeat the following substeps on all four nodes to clear the configuration:

- a. Set the environmental variables to default values:

```
set-defaults
```

- b. Save the environment:

```
saveenv
```

```
bye
```

6. Repeat the following substeps to boot all four nodes using the 9a option on the boot menu.

- a. At the LOADER prompt, launch the boot menu:

```
boot_ontap menu
```

- b. At the boot menu, select option “9a” to reboot the controller.

7. Boot each of the four nodes to Maintenance mode using option “5” on the boot menu.

8. Record the system ID and from each of the four nodes:

```
sysconfig
```

9. Repeat the following steps on node_A_1-IP and node_B_1-IP.

- a. Assign ownership of all disks local to each site:

```
disk assign adapter.xx.*
```

b. Repeat the previous step for each HBA with attached drive shelves on node_A_1-IP and node_B_1-IP.

10. Repeat the following steps on node_A_1-IP and node_B_1-IP to clear the mailbox region on each local disk.

a. Destroy the mailbox region on each disk:

```
mailbox destroy local``mailbox destroy partner
```

11. Halt all four controllers:

```
halt
```

12. On each controller, display the boot menu:

```
boot_ontap menu
```

13. On each of the four controllers, clear the configuration:

```
wipeconfig
```

When the wipeconfig operation completes, the node automatically returns to the boot menu.

14. Repeat the following substeps to again boot all four nodes using the 9a option on the boot menu.

a. At the LOADER prompt, launch the boot menu:

```
boot_ontap menu
```

b. At the boot menu, select option “9a” to reboot the controller.

c. Let the controller module complete booting before moving to the next controller module.

After “9a” completes, the nodes automatically return to the boot menu.

15. Power off the controllers.

Verifying the health of the MetroCluster FC configuration

You must verify the health and connectivity of the MetroCluster FC configuration prior to performing the transition

This task is performed on the MetroCluster FC configuration.

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

```
storage switch show
```

- g. Run Config Advisor.

[NetApp Downloads: Config Advisor](#)

- h. 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 nodes are in non-HA mode:

```
storage failover show
```

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.

Transitioning the MetroCluster FC nodes

You must gather information from the existing MetroCluster FC nodes, send an autosupport message announcing the start of maintenance, and transition the nodes.

Gathering information from the existing controller modules before the transition

Before transitioning, you must gather information for each of the nodes.

This task is performed on the existing nodes:

- node_A_1-FC
- node_B_1-FC

1. Gather the output for the commands in the following table.

Category	Commands	Notes
License	system license show	
Shelves and numbers of disks in each shelf and flash storage details and memory and NVRAM and and network cards	system node run -node node_name sysconfig	
Cluster network and node management LIFs	system node run -node node_name sysconfig network interface show -role "cluster,node-mgmt,data"	
SVM information	vserver show	
Protocol information	nfs show iscsi show cifs show	
Physical ports	network port show -node node_name -type physical network port show	
Failover Groups	network interface failover-groups show -vserver vserver_name	Record the names and ports of failover groups that are not clusterwide.
VLAN configuration	network port vlan show -node node_name	Record each network port and VLAN ID pairing.
Interface group configuration	network port ifgrp show -node node_name -instance	Record the names of the interface groups and the ports assigned to them.
Broadcast domains	network port broadcast-domain show	
IPspace	network ipspace show	
Volume info	volume show and volume show -fields encrypt	
Aggregate Info	storage aggregate show and storage aggr encryption show andstorage aggregate object-store show	
Disk ownership information	storage aggregate show and storage aggr encryption show andstorage aggregate object-store show	
Encryption	storage failover mailbox-disk show and security key-manager backup show	Also preserve the passphrase used to enable key-manager. In the case of external key-manager you will need the authentication information for the client and server.
Encryption	security key-manager show	

Category	Commands	Notes
Encryption	security key-manager external show	
Encryption	systemshell local kenv kmip.init.ipaddr ip-address	
Encryption	systemshell local kenv kmip.init.netmask netmask	
Encryption	systemshell local kenv kmip.init.gateway gateway	
Encryption	systemshell local kenv kmip.init.interface interface	

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. This prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

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.

Transitioning, shutting down, and removing the MetroCluster FC nodes

In addition to issuing commands on the MetroCluster FC nodes, this task includes physical uncabling and removal of the controller modules at each site.

This task must be performed on each of the old nodes:

- `node_A_1-FC`
- `node_B_1-FC`

Steps

1. Stop all client traffic.
2. On either of the MetroCluster FC nodes, for example `node_A_1-FC`, enable transition.
 - a. Set the advanced privilege level: `set -priv advanced`
 - b. Enable transition: `metrocluster transition enable -transition-mode disruptive`

- c. Return to admin mode: `set -priv admin`

3. Unmirror the root aggregate by deleting the remote plex of the root aggregates.

- a. Identify the root aggregates: `storage aggregate show -root true`
- b. Display the pool1 aggregates: `storage aggregate plex show -pool 1`
- c. Offline and delete the remote plex of the root aggregate:
`aggr plex offline <root-aggregate> -plex <remote-plex-for-root-aggregate>`
`aggr plex delete <root-aggregate> -plex <remote-plex-for-root-aggregate>`

For example:

```
# aggr plex offline aggr0_node_A_1-FC_01 -plex remoteplex4
```

```
# aggr plex delete aggr0_node_A_1-FC_01 -plex remoteplex4
```

4. Confirm the mailbox count, disk autoassign, and transition mode before proceeding using the following commands on each controller:

- a. Set the advanced privilege level: `set -priv advanced`
- b. Confirm that only three mailbox drives are shown for each controller module: `storage failover mailbox-disk show`
- c. Return to admin mode: `set -priv admin`
- d. Confirm that the transition mode is disruptive: `metrocluster transition show`

5. Check for any broken disks: `disk show -broken`

6. Remove or replace any broken disks

7. Confirm aggregates are healthy by using the following commands on node_A_1-FC and node_B_1-FC:

`storage aggregate show`

`storage aggregate plex show`

The storage aggregate show command indicates that the root aggregate is unmirrored.

8. Check for any VLANs or interface groups:

`network port ifgrp show`

`network port vlan show`

If none are present, skip the following two steps.

9. Display the list of LIFs using VLANs or ifgrps:

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

```
network port show -type if-group | vlan
```

10. Remove any VLANs and interface groups.

You must perform these steps for all LIFs in all SVMs, including those SVMs with the -mc suffix.

- a. Move any LIFs using the VLANs or interface groups to an available port: `network interface modify -vserver vserver-name -lif lif_name -home- port port`
- b. Display the LIFs that are not on their home ports: `network interface show -is-home false`
- c. Revert all LIFs to their respective home ports: `network interface revert -vserver vserver_name -lif lif_name`
- d. Verify that all LIFs are on their home ports: `network interface show -is-home false`
No LIFs should appear in the output.
- e. Remove VLAN and ifgrp ports from broadcast domain: `network port broadcast-domain remove-ports -ipspace ipspace -broadcast-domain broadcast-domain-name -ports nodename:portname,nodename:portname,...`
- f. Verify that all the vlan and ifgrp ports are not assigned to a broadcast domain: `network port show -type if-group | vlan`
- g. Delete all VLANs: `network port vlan delete -node nodename -vlan-name vlan-name`
- h. Delete interface groups: `network port ifgrp delete -node nodename -ifgrp ifgrp-name`

11. Move any LIFs as required to resolve conflicts with the MetroCluster IP interface ports.

You must move the LIFs identified in step 1 of [Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes](#).

- a. Move any LIFs hosted on the desired port to another port: `network interface modify -lif lifname -vserver vserver-name -home-port new-homeport``network interface revert -lif lifname -vserver vservername`
- b. If necessary, move the destination port to an appropriate IPspace and broadcast domain. `network port broadcast-domain remove-ports -ipspace current-ipspace -broadcast-domain current-broadcast-domain -ports controller-name:current-port``network port broadcast-domain add-ports -ipspace new-ipspace -broadcast-domain new-broadcast-domain -ports controller-name:new-port`
12. Halt the MetroCluster FC controllers (node_A_1-FC and node_B_1-FC): `system node halt`
13. At the LOADER prompt, synchronize the hardware clocks between the FC and IP controller modules.
 - a. On the old MetroCluster FC node (node_A_1-FC), display the date: `show date`
 - b. On the new MetroCluster IP controllers (node_A_1-IP and node_B_1-IP), set the date shown on original controller: `set date mm/dd/yy`
 - c. On the new MetroCluster IP controllers (node_A_1-IP and node_B_1-IP), verify the date: `show date`
14. Halt and power off the MetroCluster FC controller modules (node_A_1-FC and node_B_1-FC), FC-to-SAS bridges (if present), FC switches (if present) and each storage shelf connected to these nodes.
15. Disconnect the shelves from the MetroCluster FC controllers and document which shelves are local

storage to each cluster.

16. If the configuration uses FC-to-SAS bridges or FC back-end switches, disconnect and remove them.

Remove FC-to-SAS bridges

- Identify the bridges:

```
system bridge show
```

- Remove the bridges:

```
system bridge remove -name <bridge_name>
```

- Confirm the bridges are removed:

```
system bridge show
```

The following example shows that the bridges are removed:

Example

```
cluster1::> system bridge remove -name ATTO_10.226.197.16
cluster1::> system bridge show

Is      Monitor
Bridge   Symbolic Name Vendor  Model      Bridge WWN
Monitored Status
-----
-----
ATTO_FibreBridge6500N_1
      Bridge Number 16
                  Atto      FibreBridge 6500N
                                2000001086603824
false   -
ATTO_FibreBridge6500N_2
      Not Set        Atto      FibreBridge 6500N
                                20000010866037e8
false   -
ATTO_FibreBridge6500N_3
      Not Set        Atto      FibreBridge 6500N
                                2000001086609e0e
false   -
ATTO_FibreBridge6500N_4
      Not Set        Atto      FibreBridge 6500N
                                2000001086609c06
false   -
4 entries were displayed.
```

Remove FC switches

a. Identify the switches:

```
system switch fibre-channel show
```

b. Remove the switches:

```
system switch fibre-channel remove -switch-name <switch_name>
```

c. Confirm the switches are removed:

```
system switch fibre-channel show
```

Example

```
cluster1::> system switch fibre-channel show
                           Symbolic                         Is
Monitor
  Switch      Name      Vendor  Model      Switch WWN
Monitored Status
-----
-----
Cisco_10.226.197.34
  mcc-cisco-8Gb-fab-4
    Cisco    DS-C9148-16P-K9
                                         2000547fee78f088
  true      ok
  mcc-cisco-8Gb-fab-1
    mcc-cisco-8Gb-fab-1
      Cisco    -
  false      -
  mcc-cisco-8Gb-fab-2
    mcc-cisco-8Gb-fab-2
      Cisco    -
  false      -
  mcc-cisco-8Gb-fab-3
    mcc-cisco-8Gb-fab-3
      Cisco    -
  false      -
  4 entries were displayed.

cluster1::> system switch fibre-channel remove -switch-name
Cisco_10.226.197.34
cluster1::> system switch fibre-channel show
                           Symbolic                         Is
Monitor
  Switch      Name      Vendor  Model      Switch WWN
Monitored Status
-----
-----
  mcc-cisco-8Gb-fab-4
    mcc-cisco-8Gb-fab-4
      Cisco
      -
  false      -
  mcc-cisco-8Gb-fab-1
    mcc-cisco-8Gb-fab-1
      Cisco    -
  false      -
  mcc-cisco-8Gb-fab-2
```

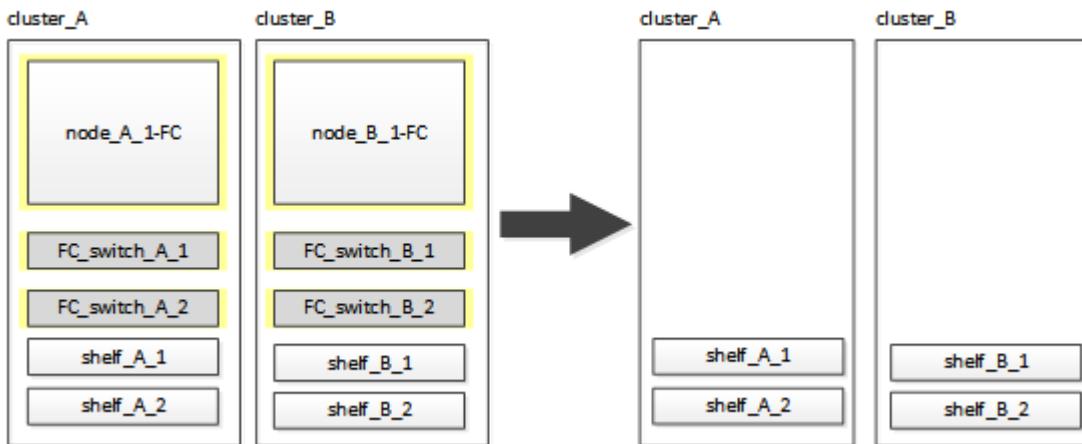
```

mcc-cisco-8Gb-fab-2
Cisco      -
false      -
mcc-cisco-8Gb-fab-3
Cisco      -
false      -
4 entries were displayed
cluster1::>

```

17. In Maintenance mode on the MetroCluster FC nodes (node_A_1-FC and node_B_1-FC), confirm no disks are connected: `disk show -v`
18. Power down and remove the MetroCluster FC nodes.

At this point, the MetroCluster FC controllers have been removed and the shelves are disconnected from all controllers.



Connecting the MetroCluster IP controller modules

You must add the four new controller modules and any additional storage shelves to the configuration. The new controller modules are added two-at-a-time.

Setting up the new controllers

You must rack and cable the new MetroCluster IP controllers to the storage shelves previously connected to the MetroCluster FC controllers.

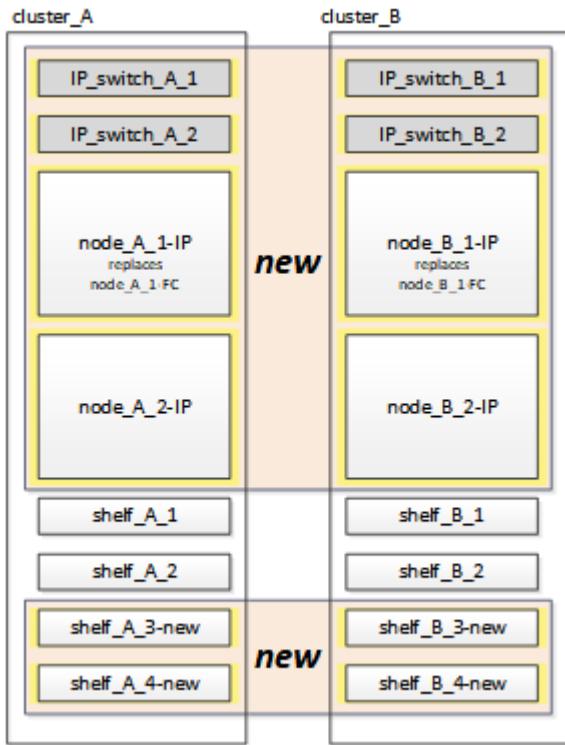
About this task

These steps must be performed on each of the MetroCluster IP nodes.

- node_A_1-IP
- node_A_2-IP
- node_B_1-IP

- node_B_2-IP

In the following example, two additional storage shelves are added at each site to provide storage to accommodate the new controller modules.



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. Rack the new equipment: controllers, storage shelves, and IP switches.

Do not cable the storage shelves or IP switches at this time.

4. Connect the power cables and management console connection to the controllers.
5. Verify that all storage shelves are powered off.
6. Verify that no drives are connected by performing the following steps on all four nodes:

- a. At the LOADER prompt, launch the boot menu:

```
boot_ontap maint
```

- b. Verify that no drives are connected:

```
disk show -v
```

The output should show no drives.

- c. Halt the node:

```
halt
```

7. Boot all four nodes using the 9a option on the boot menu.

a. At the LOADER prompt, launch the boot menu:

```
boot_ontap menu
```

b. At the boot menu, select option “9a” to reboot the controller.

c. Let the controller module complete booting before moving to the next controller module.

After “9a” completes, the nodes automatically return to the boot menu.

8. Cable the storage shelves.

Refer to the controller installation and setup procedures for your model for cabling information.

[ONTAP Hardware Systems Documentation](#)

9. Cable the controllers to the IP switches as described in [Cabling the IP switches](#).

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

Follow the steps for your switch vendor:

- [Reset the Broadcom IP switch to factory defaults](#)
- [Reset the Cisco IP switch to factory defaults](#)
- [Reset the NVIDIA IP SN2100 switch to factory defaults](#)

11. Download and install the RCF files.

Follow the steps for your switch vendor:

- [Download and install the Broadcom IP RCF files](#)
- [Download and install the Cisco IP RCF files](#)
- [Download and install the NVIDIA RCF files](#)

12. Turn on power to the first new controller (node_A_1-IP) and press Ctrl-C to interrupt the boot process and display the LOADER prompt.

13. Boot the controller to Maintenance mode:

```
boot_ontap_maint
```

14. Display the system ID for the controller:

```
sysconfig -v
```

15. Confirm that the shelves from the existing configuration are visible from the new MetroCluster IP node:

```
storage show shelf``disk show -v
```

16. Halt the node:

```
halt
```

17. Repeat the preceding steps on the other node at the partner site (site_B).

Connecting and booting up node_A_1-IP and node_B_1-IP

After connecting the MetroCluster IP controllers and IP switches, you transition and boot up node_A_1-IP and node_B_1-IP.

Bringing up node_A_1-IP

You must boot the node with the correct transition option.

Steps

1. Boot node_A_1-IP to the boot menu:

```
boot_ontap menu
```

2. Issue the following command at the boot menu prompt to initiate transition:

```
boot_after_mcc_transition
```

- This command reassigns all the disks owned by node_A_1-FC to node_A_1-IP.
 - node_A_1-FC disks are assigned to node_A_1-IP
 - node_B_1-FC disks are assigned to node_B_1-IP
- The command also automatically makes other required system ID reassessments so the MetroCluster IP nodes can boot to the ONTAP prompt.
- If the boot_after_mcc_transition command fails for any reason, it should be re-run from the boot menu.
 - If the following prompt is displayed, enter Ctrl-C to continue. Checking MCC DR state... [enter Ctrl-C(resume), S(status), L(link)]
 - If the root volume was encrypted, the node halts with the following message. Halting the system, because root volume is encrypted (NetApp Volume Encryption) and the key import failed. If this cluster is configured with external (KMIP) key-manager, check the health of the key servers.

```

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. Selection (1-9) ?
`boot_after_mcc_transition`
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

MetroCluster Transition: Name of the MetroCluster FC node: `node_A_1-
FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]?: y
MetroCluster Transition: Disaster Recovery partner sysid of
MetroCluster FC node node_A_1-FC: `systemID-of-node_B_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]?: y
MetroCluster Transition: Disaster Recovery partner sysid of local
MetroCluster IP node: `systemID-of-node_B_1-IP`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]?: y

```

3. If data volumes are encrypted, 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 key query -node node-name</pre> <p>For more information, see Restoring external key management encryption keys.</p>

4. If the root volume is encrypted, use the procedure in [Recovering key management if the root volume is encrypted](#).

Recovering key management if the root volume is encrypted

If the root volume is encrypted, you must use special boot commands to restore the key management.

Before you begin

You must have the passphrases gathered earlier.

Steps

1. If onboard key management is used, perform the following substeps to restore the configuration.

- a. From the LOADER prompt, display the boot menu:

```
boot_ontap menu
```

- b. Select option “(10) Set onboard key management recovery secrets” from the boot menu.

Respond as appropriate to the prompts:

```
This option must be used only in disaster recovery procedures. Are  
you sure? (y or n): y
```

```
Enter the passphrase for onboard key management: passphrase
```

```
Enter the passphrase again to confirm: passphrase
```

```
Enter the backup data: backup-key
```

The system boots to the boot menu.

- c. Enter option “6” at the boot menu.

Respond as appropriate to the prompts:

```
This will replace all flash-based configuration with the last backup  
to
```

```
disks. Are you sure you want to continue?: y
```

```
Following this, the system will reboot a few times and the following  
prompt will be available continue by saying y
```

```
WARNING: System ID mismatch. This usually occurs when replacing a  
boot device or NVRAM cards!
```

```
Override system ID? {y|n} y
```

After the reboots, the system will be at the LOADER prompt.

- d. From the LOADER prompt, display the boot menu:

```
boot_ontap menu
```

- e. Again elect option “(10) Set onboard key management recovery secrets” from the boot menu.

Respond as appropriate to the prompts:

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm: `passphrase`

Enter the backup data: `backup-key`
```

The system boots to the boot menu.

- f. Enter option “1” at the boot menu.

If the following prompt is displayed, you can press Ctrl+C to resume the process.

```
Checking MCC DR state... [enter Ctrl-C(resume), S(status), L(link)]
```

The system boots to the ONTAP prompt.

- g. Restore the onboard key management:

```
security key-manager onboard sync
```

Respond as appropriate to the prompts, using the passphrase you collected earlier:

```
cluster_A::> security key-manager onboard sync
Enter the cluster-wide passphrase for onboard key management in
Vserver "cluster_A":: passphrase
```

2. If external key management is used, perform the following substeps to restore the configuration.

- a. Set the required 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
```

- b. From the LOADER prompt, display the boot menu:

```
boot_ontap menu
```

- c. Select option “(11) Configure node for external key management” from the boot menu.

The system boots to the boot menu.

d. Enter option “6” at the boot menu.

The system boots multiple times. You can respond affirmatively when prompted to continue the boot process.

After the reboots, the system will be at the LOADER prompt.

e. Set the required 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
```

f. From the LOADER prompt, display the boot menu:

```
boot_ontap menu
```

g. Again select option “(11) Configure node for external key management” from the boot menu and respond to the prompts as required.

The system boots to the boot menu.

h. Restore the external key management:

```
security key-manager external restore
```

Creating the network configuration

You must create a network configuration that matches the configuration on the FC nodes. This is because the MetroCluster IP node replays the same configuration when it boots, which means that when node_A_1-IP and node_B_1-IP boot, ONTAP will try to host LIFs on the same ports that were used on node_A_1-FC and node_B_1-FC respectively.

About this task

As you create the network configuration, use the plan made in [Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes](#) to assist you.



Additional configuration may be needed to bring up data LIFs after the MetroCluster IP nodes have been configured.

Steps

1. Verify that all cluster ports are in the appropriate broadcast domain:

The cluster IPSpace and cluster broadcast domain are required in order to create cluster LIFs

a. View the IP spaces:

```
network ipspace show
```

- b. Create IP spaces and assign cluster ports as needed.

[Configuring IPspaces \(cluster administrators only\)](#)

- c. View the broadcast domains:

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

- d. Add any cluster ports to a broadcast domain as needed.

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

- e. 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](#)

2. Verify that MTU settings are set correctly for the ports and broadcast domain and make changes using the following commands:

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

```
network port broadcast-domain modify -broadcast-domain bcastdomainname -mtu mtu-value
```

Setting up cluster ports and cluster LIFs

You must set up cluster ports and LIFs. The following steps need to be performed on the site A nodes which were booted up with root aggregates.

Steps

1. Identify the list of LIFs using the desired Cluster port:

```
network interface show -curr-port portname
```

```
network interface show -home-port portname
```

2. For each cluster port, change the home port of any of the LIFs on that port to another port,

- a. Enter advanced privilege mode and enter "y" when prompted to continue:

```
set priv advanced
```

- b. If the LIF being modified is a data LIF:

```
vserver config override -command "network interface modify -lif lname -vserver vservername -home-port new-datahomeport"
```

- c. If the LIF is not a data LIF:

```
network interface modify -lif lname -vserver vservername -home-port new-
```

```
datahomeport
```

- d. Revert the modified LIFs to their home port:

```
network interface revert * -vserver vserver_name
```

- e. Verify that there are no LIFs on the cluster port:

```
network interface show -curr-port portname
```

```
network interface show -home-port portname
```

- f. Remove the port from the current broadcast domain:

```
network port broadcast-domain remove-ports -ipspace ipspacename -broadcast -domain bcastdomainname -ports node_name:port_name
```

- g. Add the port to the cluster IPspace and broadcast domain:

```
network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports node_name:port_name
```

- h. Verify that the port's role has changed: network port show

- i. Repeat these substeps for each cluster port.

- j. Return to admin mode:

```
set priv admin
```

3. Create cluster LIFs on the new cluster ports:

- a. For autoconfiguration using link-local address for cluster LIF, use the following command:

```
network interface create -vserver Cluster -lif cluster_lifname -service -policy default-cluster -home-node alname -home-port clusterport -auto true
```

- b. To assign static IP address for the cluster LIF, use the following command:

```
network interface create -vserver Cluster -lif cluster_lifname -service -policy default-cluster -home-node alname -home-port clusterport -address ip-address -netmask netmask -status-admin up
```

Verifying LIF configuration

The node management LIF, cluster management LIF and intercluster LIF will still be present after the storage movement from the old controller. If necessary, you must move LIFs to appropriate ports.

Steps

1. Verify whether the management LIF and cluster management LIFs are on the desired port already:

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

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

If the LIFs are on the desired ports, you can skip the rest of the steps in this task and proceed to the next task.

2. For each node, cluster management, or intercluster LIFs that are not on the desired port, change the home port of any of the LIFs on that port to another port.

- a. Repurpose the desired port by moving any LIFs hosted on desired port to another port:

```
vserver config override -command "network interface modify -lif lifname -vserver vservername -home-port new-datahomeport"
```

- b. Revert the modified LIFs to their new home port:

```
vserver config override -command "network interface revert -lif lifname -vserver vservername"
```

- c. If the desired port is not in the right IPspace and broadcast domain, remove the port from the current IPspace and broadcast domain:

```
network port broadcast-domain remove-ports -ipspace current-ipspace -broadcast-domain current-broadcast-domain -ports controller-name:current-port
```

- d. Move the desired port to the right IPspace and broadcast domain:

```
network port broadcast-domain add-ports -ipspace new-ipspace -broadcast-domain new-broadcast-domain -ports controller-name:new-port
```

- e. Verify that the port's role has changed:

```
network port show
```

- f. Repeat these substeps for each port.

3. Move node, cluster management LIFs, and intercluster LIF to the desired port:

- a. Change the LIF's home port:

```
network interface modify -vserver vserver -lif node_mgmt -home-port port -home-node homenode
```

- b. Revert the LIF to its new home port:

```
network interface revert -lif node_mgmt -vserver vservername
```

- c. Change the cluster management LIF's home port:

```
network interface modify -vserver vserver -lif cluster-mgmt-LIF-name -home-port port -home-node homenode
```

- d. Revert the cluster management LIF to its new home port:

```
network interface revert -lif cluster-mgmt-LIF-name -vserver vservername
```

- e. Change the intercluster LIF's home port:

```
network interface modify -vserver vserver -lif intercluster-lif-name -home -node nodename -home-port port
```

- f. Revert the intercluster LIF to its new home port:

```
network interface revert -lif intercluster-lif-name -vserver vservername
```

Bringing up node_A_2-IP and node_B_2-IP

You must bring up and configure the new MetroCluster IP node at each site, creating an HA pair in each site.

Bringing up node_A_2-IP and node_B_2-IP

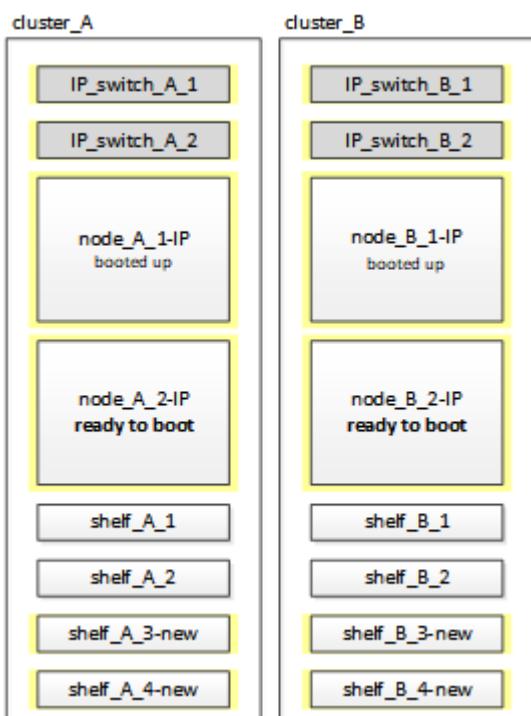
You must boot the new controller modules one at a time using the correct option at the boot menu.

About this task

In these steps, you boot up the two brand new nodes, expanding what had been a two-node configuration into a four-node configuration.

These steps are performed on the following nodes:

- node_A_2-IP
- node_B_2-IP



Steps

1. Boot the new nodes using boot option “9c”.

```
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. Selection (1-9) ? 9c
```

The node initializes and boots to the node setup wizard, 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. .  
. .
```

If option "9c" does not succeed, take the following steps to avoid possible data loss:

- Do not attempt to run option 9a.
- Physically disconnect the existing shelves that contain data from the original MetroCluster FC configuration (shelf_A_1, shelf_A_2, shelf_B_1, shelf_B_2).
- Contact technical support, referencing the KB article [MetroCluster FC to IP transition - Option 9c Failing](#).

[NetApp Support](#)

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

```
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. Verify that the storage failover mode is set to HA:

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

If the mode is not HA, set it:

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

You must then reboot the node for the change to take effect.

5. 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						
Node	Port	IPspace	Broadcast	Domain	Link	MTU
(Mbps) Speed						
cluster01-01	e0a	Cluster	Cluster		up	1500
	e0b	Cluster	Cluster		up	1500
	e0c	Default	Default		up	1500
	e0d	Default	Default		up	1500
	e0e	Default	Default		up	1500
	e0f	Default	Default		up	1500
cluster01-02	e0a	Cluster	Cluster		up	1500
	e0b	Cluster	Cluster		up	1500
	e0c	Default	Default		up	1500
	e0d	Default	Default		up	1500
	e0e	Default	Default		up	1500
	e0f	Default	Default		up	1500

6. Exit the Node Setup wizard:

```
exit
```

7. Log into the admin account using the admin user name.

8. Join the existing cluster using the Cluster Setup wizard.

```

:> 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
```

10. Disable disk autoassignment:

```
storage disk option modify -autoassign off -node node_A_2-IP
```

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	<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 key query -node node-name</pre> <p>For more information, see Restoring external key management encryption keys.</p>

12. Repeat the above steps on the second new controller module (node_B_2-IP).

Verifying MTU settings

Verify that MTU settings are set correctly for the ports and broadcast domain and make changes.

Steps

1. Check the MTU size used in the cluster broadcast domain:

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

2. If necessary, update the MTU size as needed:

```
network port broadcast-domain modify -broadcast-domain bcast-domain-name -mtu mtu-size
```

Configuring intercluster LIFs

Configure the intercluster LIFs required for cluster peering.

This task must be performed on both of the new nodes, *node_A_2-IP* and *node_B_2-IP*.

Step

1. Configure the intercluster LIFs. See [Configuring intercluster LIFs](#)

Verifying cluster peering

Verify that *cluster_A* and *cluster_B* are peered and nodes on each cluster can communicate with each other.

Steps

1. Verify the cluster peering relationship:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node          cluster-Name          Node-Name
              Ping-Status          RDB-Health Cluster-Health  Avail...
-----
-----
node_A_1-IP
          cluster_B          node_B_1-IP
          Data: interface_reachable
          ICMP: interface_reachable  true      true      true
                  node_B_2-IP
          Data: interface_reachable
          ICMP: interface_reachable  true      true      true
node_A_2-IP

image:.../media/transition_2n_booting_a_2_and_b_2.png["Booting new IP
nodes during transition"]
          Data: interface_reachable
          ICMP: interface_reachable  true      true      true
                  node_B_2-IP
          Data: interface_reachable
          ICMP: interface_reachable  true      true      true
```

2. Ping to check that the peer addresses are reachable:

```
cluster peer ping -originating-node local-node -destination-cluster remote-cluster-name
```

Configuring the new nodes and completing transition

With the new nodes added, you must complete the transition steps and configure the MetroCluster IP nodes.

Configuring the MetroCluster IP nodes and disabling transition

You must implement the MetroCluster IP connections, refresh the MetroCluster configuration, and disable transition mode.

Steps

1. Form the new nodes into a DR group by issuing the following commands from controller node_A_1-IP:

```
metrocluster configuration-settings dr-group create -partner-cluster
<peer_cluster_name> -local-node <local_controller_name> -remote-node
<remote_controller_name>
```

```
metrocluster configuration-settings dr-group show
```

2. Create MetroCluster IP interfaces (node_A_1-IP, node_A_2-IP, node_B_1-IP, node_B_2-IP)—two interfaces need to be created per controller; eight interfaces in total:



Do not use 169.254.17.x or 169.254.18.x IP addresses when you create MetroCluster IP interfaces to avoid conflicts with system auto-generated interface IP addresses in the same range.

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <controller_name> -home-port <port_name> -address
<ip_address> -netmask <netmask_address> -vlan-id <vlan_id>
```

```
metrocluster configuration-settings interface show
```

Certain platforms use a VLAN for the MetroCluster IP interface. By default, each of the two ports use a different VLAN: 10 and 20.

If supported, 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.

The following platforms do **not** support the `-vlan-id` parameter:

- FAS8200 and AFF A300
- AFF A320
- FAS9000 and AFF A700
- AFF C800, ASA C800, AFF A800 and ASA A800

All other platforms support the `-vlan-id` parameter.

The default and valid VLAN assignments depend on whether the platform supports the `-vlan-id` parameter:

Platforms that support `-vlan-id`

Default VLAN:

- When the `-vlan-id` parameter is not specified, the interfaces are created with VLAN 10 for the "A" ports and VLAN 20 for the "B" ports.
- The VLAN specified must match the VLAN selected in the RCF.

Valid VLAN ranges:

- Default VLAN 10 and 20
- VLANs 101 and higher (between 101 and 4095)

Platforms that do not support `-vlan-id`

Default VLAN:

- Not applicable. The interface does not require a VLAN to be specified on the MetroCluster interface. The switch port defines the VLAN that is used.

Valid VLAN ranges:

- All VLANs not explicitly excluded when generating the RCF. The RCF alerts you if the VLAN is invalid.

3. Perform the MetroCluster connect operation from controller node_A_1-IP to connect the MetroCluster sites — this operation can take a few minutes to complete:

```
metrocluster configuration-settings connection connect
```

4. Verify that the remote cluster disks are visible from each controller via the iSCSI connections:

```
disk show
```

You should see the remote disks belonging to the other nodes in the configuration.

5. Mirror the root aggregate for node_A_1-IP and node_B_1-IP:

```
aggregate mirror -aggregate root-aggr
```

6. Assign disks for node_A_2-IP and node_B_2-IP.

Pool 1 disk assignments were already made for node_A_1-IP and node_B_1-IP when the `boot_after_mcc_transition` command was issued at the boot menu.

a. Issue the following commands on node_A_2-IP:

```
disk assign disk1disk2disk3 ... diskn -sysid node_B_2-IP-controller-sysid
-pool 1 -force
```

b. Issue the following commands on node_B_2-IP:

```
disk assign disk1disk2disk3 ... diskn -sysid node_A_2-IP-controller-sysid
```

```
-pool 1 -force
```

7. Confirm ownership has been updated for the remote disks:

```
disk show
```

8. If necessary, refresh the ownership information using the following commands:

- Go to advanced privilege mode and enter y when prompted to continue:

```
set priv advanced
```

- Refresh disk ownership:

```
disk refresh-ownership controller-name
```

- Return to admin mode:

```
set priv admin
```

9. Mirror the root aggregates for node_A_2-IP and node_B_2-IP:

```
aggregate mirror -aggregate root-aggr
```

10. Verify that the aggregate re-synchronization has completed for root and data aggregates:

```
aggr show``aggr plex show
```

The resync can take some time but must complete before proceeding with the following steps.

11. Refresh the MetroCluster configuration to incorporate the new nodes:

- Go to advanced privilege mode and enter y when prompted to continue:

```
set priv advanced
```

- Refresh the configuration:

If you have configured...	Issue this command...
A single aggregate in each cluster:	metrocluster configure -refresh true -allow-with-one-aggregate true
More than a single aggregate in each cluster	metrocluster configure -refresh true

- Return to admin mode:

```
set priv admin
```

12. Disable MetroCluster transition mode:

- Enter advanced privilege mode and enter "y" when prompted to continue:

```
set priv advanced
```

- b. Disable transition mode:

```
metrocluster transition disable
```

- c. Return to admin mode:

```
set priv admin
```

Setting up data LIFs on the new nodes

You must configure data LIFs on the new nodes, node_A_2-IP and node_B_2-IP.

You must add any new ports available on new controllers to a broadcast domain if not already assigned to one. If required, create VLANs or interface groups on the new ports. See [Network management](#)

1. Identify the current port usage and broadcast domains:

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

2. Add ports to broadcast domains and VLANs as necessary.

- a. View the IP spaces:

```
network ipspace show
```

- b. Create IP spaces and assign data ports as needed.

[Configuring IPspaces \(cluster administrators only\)](#)

- c. View the broadcast domains:

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

- d. Add any data ports to a broadcast domain as needed.

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

- e. 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](#)

3. Verify that the LIFs are hosted on the appropriate node and ports on the MetroCluster IP nodes (including the SVM with -mc vserver) as needed.

See the information gathered in [Creating the network configuration](#).

- a. Check the home port of the LIFs:

```
network interface show -field home-port
```

- b. If necessary, modify the LIF configuration:

```
vserver config override -command "network interface modify -vserver
<svm_name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
<new_node_name>
```

- c. Revert the LIFs to their home ports:

```
network interface revert * -vserver <svm_name>
```

Bringing up the SVMs

Due to the changes in LIF configuration, you must restart the SVMs on the new nodes.

Steps

1. Check the state of the SVMs:

```
metrocluster vserver show
```

2. Restart the SVMs on cluster_A that do not have an "-mc" suffix:

```
vserver start -vserver <svm_name> -force true
```

3. Repeat the previous steps on the partner cluster.

4. Check that all SVMs are in a healthy state:

```
metrocluster vserver show
```

5. Verify that all data LIFs are online:

```
network interface show
```

Moving a system volume to the new nodes

To improve resiliency, a system volume should be moved from controller node_A_1-IP to controller node_A_2-IP, and also from node_B_1-IP to node_B_2-IP. You must create a mirrored aggregate on the destination node for the system volume.

About this task

System volumes have the name form "MDV_CRS_*_A" or "MDV_CRS_*_B." The designations "_A" and "_B" are unrelated to the site_A and site_B references used throughout this section; e.g., MDV_CRS_*_A is not associated with site_A.

Steps

1. Assign at least three pool 0 and three pool 1 disks each for controllers node_A_2-IP and node_B_2-IP as needed.
2. Enable disk auto-assignment.
3. Move the _B system volume from node_A_1-IP to node_A_2-IP using the following steps from site_A.
 - a. Create a mirrored aggregate on controller node_A_2-IP to hold the system volume:

```
aggr create -aggregate new_node_A_2-IP_aggr -diskcount 10 -mirror true -node
node_A_2-IP
```

```
aggr show
```

The mirrored aggregate requires five pool 0 and five pool 1 spare disks owned by controller node_A_2-IP.

The advanced option, “-force-small-aggregate true” can be used to limit disk use to 3 pool 0 and 3 pool 1 disks, if disks are in short supply.

- b. List the system volumes associated with the admin SVM:

```
vserver show
```

```
volume show -vserver <admin_svm_name>
```

You should identify volumes contained by aggregates owned by site_A. The site_B system volumes will also be shown.

4. Move the MDV_CRS_*_B system volume for site_A to the mirrored aggregate created on controller node_A_2-IP

- a. Check for possible destination aggregates:

```
volume move target-aggr show -vserver <admin_svm_name> -volume MDV_CRS_*_B
```

The newly created aggregate on node_A_2-IP should be listed.

- b. Move the volume to the newly created aggregate on node_A_2-IP:

```
set advanced
```

```
volume move start -vserver <admin_svm_name> -volume MDV_CRS_*_B -destination -aggregate new_node_A_2-IP_aggr -cutover-window 40
```

- c. Check status for the move operation:

```
volume move show -vserver <admin_svm_name> -volume MDV_CRS_*_B
```

- d. When the move operation complete, verify that the MDV_CRS_*_B system is contained by the new aggregate on node_A_2-IP:

```
set admin
```

```
volume show -vserver <admin_svm_name>
```

5. Repeat the above steps on site_B (node_B_1-IP and node_B_2-IP).

Returning the system to normal operation

You must perform final configuration steps and return the MetroCluster configuration to normal operation.

Verifying MetroCluster operation and assigning drives after transition

You must verify that the MetroCluster is operating correctly and assign drives to the second pair of new nodes

(node_A_2-IP and node_B_2-IP).

1. Confirm that the MetroCluster configuration-type is IP-fabric: `metrocluster show`
2. Perform a MetroCluster check.
 - a. Issue the following command: `metrocluster check run`
 - b. Display the results of the MetroCluster check: `metrocluster check show`
3. Confirm that the DR group with the MetroCluster IP nodes is configured: `metrocluster node show`
4. Create and mirror additional data aggregates for controllers node_A_2-IP and node_B_2-IP at each site as needed.

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*.

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

For further information on license replacements, see the Knowledge Base article [Post Motherboard Replacement Process to update Licensing on a AFF/FAS system](#).

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.

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

Completing configuration of the nodes

There are miscellaneous configuration steps that can be performed prior to completing the procedures. Some of these steps are optional.

1. Configure the service processor: `system service-processor network modify`
2. Set up autosupport on the new nodes: `system node autosupport modify`
3. The controllers can be optionally renamed as part of the transition. The following command is used to rename a controller: `system node rename -node <old-name> -newname <new-name>`

The renaming operation can take a few minutes to complete. Confirm that any name changes have propagated to each node prior to continuing with other steps using the `system show -fields node` command.

4. Configure a monitoring service as desired.

Considerations for Mediator

Configure ONTAP Mediator for unplanned automatic switchover

Tiebreaker Software installation and configuration

Sending a custom AutoSupport message after maintenance

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

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.

Disruptively transitioning from MetroCluster FC to MetroCluster IP when retiring storage shelves (ONTAP 9.8 and later)

Beginning with ONTAP 9.8, you can disruptively transition a two-node MetroCluster FC configuration to a four-node MetroCluster IP configuration and retire the existing storage shelves. The procedure includes steps to move data from the existing drive shelves to the new configuration, and then retire the old shelves.

- This procedure is used when you plan to retire the existing storage shelves and move all data to the new shelves in the MetroCluster IP configuration.
- The existing storage shelf models must be supported by the new MetroCluster IP nodes.
- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is disruptive.
- This procedure applies only to a two-node MetroCluster FC configuration.

If you have a four-node MetroCluster FC configuration, see [Choosing your transition procedure](#).

- You must meet all requirements and follow all steps in the procedure.

Enable console logging

NetApp strongly recommends that you enable console logging on the devices that you are using and take the following actions when performing this procedure:

- Leave AutoSupport enabled during maintenance.
- Trigger a maintenance AutoSupport message before and after maintenance to disable case creation for the duration of the maintenance activity.

See the Knowledge Base article [How to suppress automatic case creation during scheduled maintenance windows](#).

- Enable session logging for any CLI session. For instructions on how to enable session logging, review the

"Logging Session Output" section in the Knowledge Base article [How to configure PuTTY for optimal connectivity to ONTAP systems](#).

Requirements for transition when retiring old shelves

Before starting the transition process, you must make sure the existing MetroCluster FC configuration meets the requirements.

- It must be a two-node fabric-attached or stretch MetroCluster configuration and all nodes must be running ONTAP 9.8 or later.

The new MetroCluster IP controller modules should be running the same version of ONTAP 9.8.

- The existing and new platforms must be a supported combination for transition.

[Supported platforms for nondisruptive transition](#)

- It must meet all requirements and cabling as described in the *MetroCluster Installation and Configuration Guides*.

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

The new configuration must also meet the following requirements:

- The new MetroCluster IP platform models must support the old storage shelf models.

[NetApp Hardware Universe](#)

- Depending on the spare disks available in the existing shelves, additional drives must be added.

This might require additional drive shelves.

You need to have additional 14 to 18 drives for each controller:

- Three pool 0 drives
- Three pool 1 drives
- Two spare drives
- Six to ten drives for the system volume

- You must ensure that the configuration, including the new nodes, does not exceed the platform limits for the configuration, including drive count, root aggregate size capacity, etc.

This information is available for each platform model at [NetApp Hardware Universe](#)

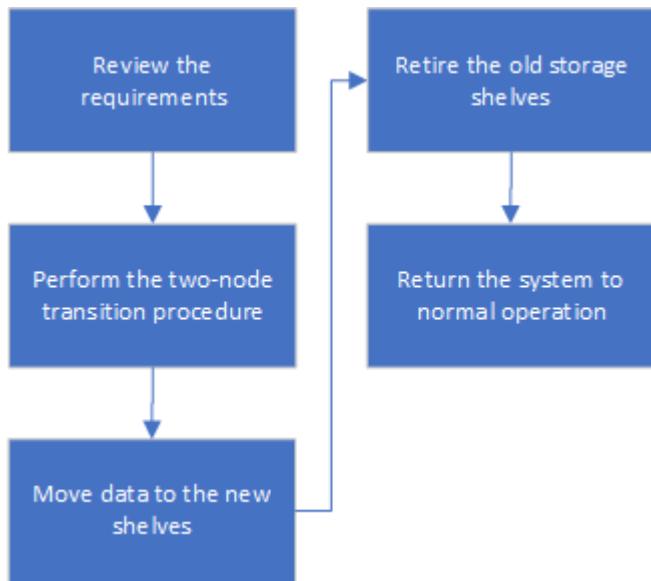
You must have remote console access for all six nodes from either MetroCluster site or plan for travel between the sites as required by the procedure.

Workflow for disruptive transition when moving data and retiring old storage shelves

You must follow the specific workflow to ensure a successful transition.

As you prepare for the transition, plan for travel between the sites. Note that after the remote nodes are racked

and cabled, you need serial terminal access to the nodes. Service Processor access is not be available until the nodes are configured.



Transitioning the configuration

You must follow the detailed transition procedure.

About this task

In the following steps you are directed to other procedures. You must perform the steps in each referenced procedure in the order given.

Steps

1. Plan port mapping using the steps in [Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes](#).
2. Prepare the MetroCluster IP controllers using the steps in [Preparing the MetroCluster IP controllers](#).
3. Verify the health of the MetroCluster FC configuration.

Perform the steps in [Verifying the health of the MetroCluster FC configuration](#).

4. Gather information from the MetroCluster FC configuration.

Perform the steps in [Gathering information from the existing controller modules before the transition](#).

5. Remove Tiebreaker monitoring, if necessary.

Perform the steps in [Removing the existing configuration from the Tiebreaker or other monitoring software](#).

6. Prepare and remove the existing MetroCluster FC nodes.

Perform the steps in [Transitioning the MetroCluster FC nodes](#).

7. Connect the new MetroCluster IP nodes.

Perform the steps in [Connecting the MetroCluster IP controller modules](#).

8. Configure the new MetroCluster IP nodes and complete transition.

Perform the steps in [Configuring the new nodes and completing transition](#).

Migrating the root aggregates

After the transition is complete, migrate the existing root aggregates leftover from the MetroCluster FC configuration to new shelves in the MetroCluster IP configuration.

About this task

This task moves the root aggregates for node_A_1-FC and node_B_1-FC to disk shelves owned by the new MetroCluster IP controllers:

Steps

1. Assign pool 0 disks on the new local storage shelf to the controller that has the root being migrated (e.g., if the root of node_A_1-FC is being migrated, assign pool 0 disks on the new shelf to node_A_1-IP)

Note that the migration *removes and does not re-create the root mirror*, so pool 1 disks do not need to be assigned before issuing the migrate command

2. Set the privilege mode to advanced:

```
set priv advanced
```

3. Migrate the root aggregate:

```
system node migrate-root -node node-name -disklist disk-id1,disk-id2,diskn  
-raid-type raid-type
```

- The node-name is the node to which the root aggregate is being migrated.
- The disk-id identifies the pool 0 disks on the new shelf.
- The raid-type is normally the same as the raid-type of the existing root aggregate.
- You can use the command `job show -id job-id-instance` to check the migration status, where job-id is the value provided when the `migrate-root` command is issued.

For example, if the root aggregate for node_A_1-FC consisted of three disks with `raid_dp`, the following command would be used to migrate root to a new shelf 11:

```
system node migrate-root -node node_A_1-IP -disklist  
3.11.0,3.11.1,3.11.2 -raid-type raid_dp
```

4. Wait until the migration operation completes and the node automatically reboots.
5. Assign pool 1 disks for the root aggregate on a new shelf directly connected to the remote cluster.
6. Mirror the migrated root aggregate.
7. Wait for the root aggregate to complete resynchronising.

You can use the `storage aggregate show` command to check the sync status of the aggregates.

8. Repeat these steps for the other root aggregate.

Migrating the data aggregates

Create data aggregates on the new shelves and use volume move to transfer the data volumes from the old shelves to the aggregates on the new shelves.

1. Move the data volumes to aggregates on the new controllers, one volume at a time.

[Creating an aggregate and moving volumes to the new nodes](#)

Retiring shelves moved from node_A_1-FC and node_A_2-FC

You retire the old storage shelves from the original MetroCluster FC configuration. These shelves were originally owned by node_A_1-FC and node_A_2-FC.

1. Identify the aggregates on the old shelves on cluster_B that need to be deleted.

In this example the following data aggregates are hosted by the MetroCluster FC cluster_B and need to be deleted: aggr_data_a1 and aggr_data_a2.



You need to perform the steps to identify, offline and delete the data aggregates on the shelves. The example is for one cluster only.

```
cluster_B::> aggr show

Aggregate      Size Available Used% State      #Vols  Nodes          RAID
Status
-----  -----  -----  -----  -----  -----  -----  -----
-----  -----
aggr0_node_A_1-FC
      349.0GB    16.83GB    95% online      1 node_A_1-IP
      raid_dp,
      mirrored,
      normal
      aggr0_node_A_2-IP
      349.0GB    16.83GB    95% online      1 node_A_2-IP
      raid_dp,
      mirrored,
      normal
      ...
8 entries were displayed.

cluster_B::>
```

2. Check if the data aggregates have any MDV_aud volumes, and delete them prior to deleting the aggregates.

You must delete the MDV_aud volumes as they cannot be moved.

3. Take each of the aggregates offline, and then delete them:

- a. Take the aggregate offline:

```
storage aggregate offline -aggregate aggregate-name
```

The following example shows the aggregate node_B_1_aggr0 being taken offline:

```
cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0
Aggregate offline successful on aggregate: node_B_1_aggr0
```

- b. Delete the aggregate:

```
storage aggregate delete -aggregate aggregate-name
```

You can destroy the plex when prompted.

The following example shows the aggregate node_B_1_aggr0 being deleted.

```
cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

4. After deleting all aggregates, power down, disconnect, and remove the shelves.

5. Repeat the above steps to retire the cluster_A shelves.

Completing transition

With the old controller modules removed, you can complete the transition process.

Step

1. Complete the transition process.

Perform the steps in [Returning the system to normal operation](#).

Disruptively transitioning when existing shelves are not supported on new controllers (ONTAP 9.8 and later)

Beginning with ONTAP 9.8, you can disruptively transition a two-node MetroCluster FC configuration and move data from the existing drive shelves even if the existing storage shelves are not supported by the new MetroCluster IP nodes.

- This procedure should only be used if the existing storage shelf models are not supported by the new MetroCluster IP platform models.
- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is disruptive.
- This procedure applies only to a two-node MetroCluster FC configuration.

If you have a four-node MetroCluster FC configuration, see [Choosing your transition procedure](#).

- You must meet all requirements and follow all steps in the procedure.

Enable console logging

NetApp strongly recommends that you enable console logging on the devices that you are using and take the following actions when performing this procedure:

- Leave AutoSupport enabled during maintenance.
- Trigger a maintenance AutoSupport message before and after maintenance to disable case creation for the duration of the maintenance activity.

See the Knowledge Base article [How to suppress automatic case creation during scheduled maintenance windows](#).

- Enable session logging for any CLI session. For instructions on how to enable session logging, review the "Logging Session Output" section in the Knowledge Base article [How to configure PuTTY for optimal connectivity to ONTAP systems](#).

Requirements for transition when shelves are not supported on the new nodes

Before starting the transition process, you must make sure the configuration meets the requirements.

Before you begin

- The existing configuration must be a two-node fabric-attached or stretch MetroCluster configuration and all nodes must be running ONTAP 9.8 or later.

The new MetroCluster IP controller modules should be running the same version of ONTAP 9.8.

- The existing and new platforms must be a supported combination for transition.

[Supported platforms for nondisruptive transition](#)

- It must meet all requirements and cabling as described in [Fabric-attached MetroCluster installation and configuration](#).
- New storage shelves provided with the new controllers (node_A_1-IP, node_A_2-IP, node_B_1-IP and node_B_2-IP) must be supported by the old controllers (node_A_1-FC and node_B_1-FC).

[NetApp Hardware Universe](#)

- The old storage shelves are **not** supported by the new MetroCluster IP platform models.

[NetApp Hardware Universe](#)

- Depending on the spare disks available in the existing shelves, additional drives must be added.

This might require additional drive shelves.

You need to have additional 14 to 18 drives for each controller:

- Three pool0 drives
- Three pool1 drives
- Two spare drives
- Six to ten drives for the system volume

- You must ensure that the configuration, including the new nodes, does not exceed the platform limits for the configuration, including drive count, root aggregate size capacity, etc.

This information is available for each platform model at *NetApp Hardware Universe*.

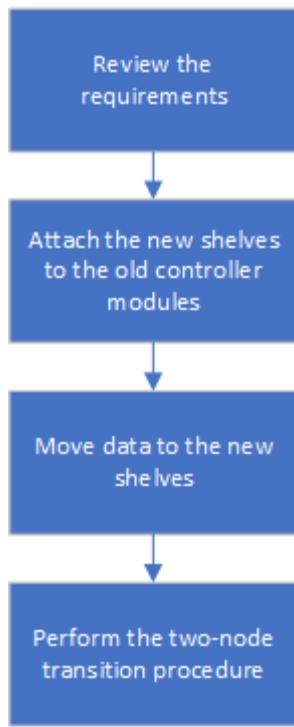
[NetApp Hardware Universe](#)

- You must have remote console access for all six nodes from either MetroCluster site or plan for travel between the sites as required by the procedure.

Workflow for disruptive transition when shelves are not supported by new controllers

If the existing shelf models are not supported by the new platform models, you must attach the new shelves to the old configuration, move data onto the new shelves, and then transition to the new configuration.

As you prepare for the transition, plan for travel between the sites. Note that after the remote nodes are racked and cabled, you need serial terminal access to the nodes. Service Processor access is not be available until the nodes are configured.



Preparing the new controller modules

You must clear the configuration and disk ownership on the new controller modules and the new storage shelves.

Steps

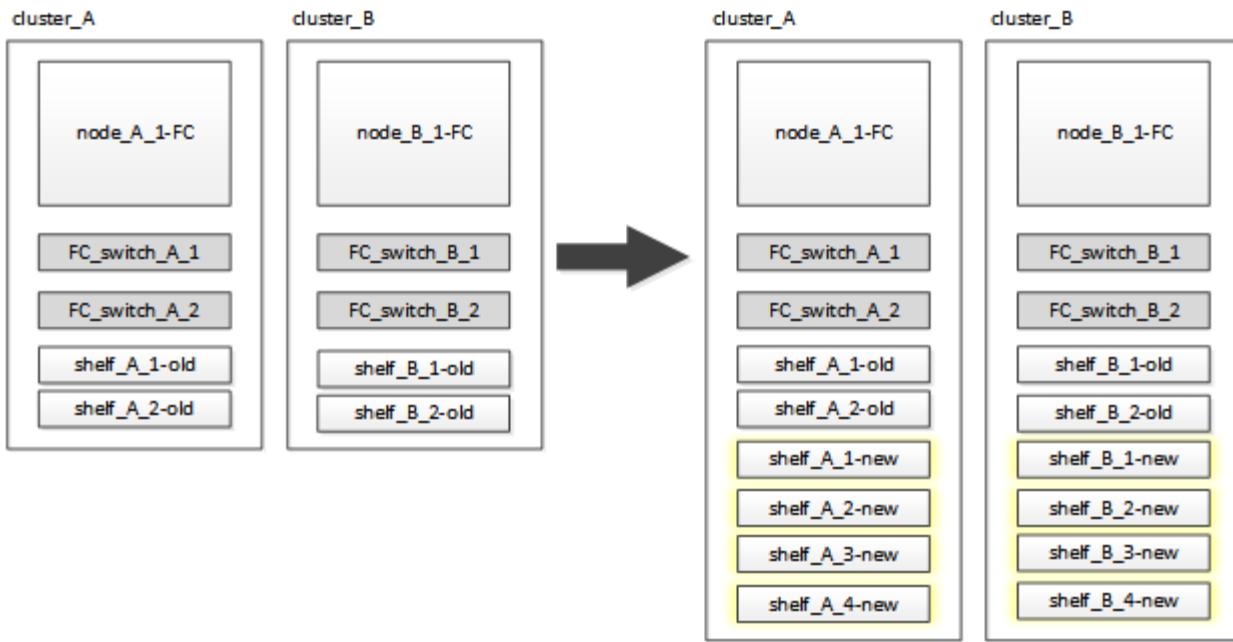
1. With the new storage shelves attached to the new MetroCluster IP controller modules, perform all the steps in [Preparing the MetroCluster IP controllers](#).
2. Disconnect the new storage shelves from the new MetroCluster IP controller modules.

Attaching the new disk shelves to the existing MetroCluster FC controllers

You must attach the new drive shelves to the existing controller modules before transitioning to a MetroCluster IP configuration.

About this task

The following illustration shows the new shelves attached to the MetroCluster FC configuration.



Steps

1. Disable disk autoassignment on node_A_1-FC and node_A_2-FC:

```
disk option modify -node node-name -autoassign off
```

This command must be issued on each node.

Disk auto-assign is disabled to avoid assignment of the shelves to be added to node_A_1-FC and node_B_1-FC. As part the transition, disks are needed for nodes node_A_1-IP and node_B_2-IP and if autoassign is allowed, disk ownership would later need to be removed before disks could be assigned to node_A_1-IP and node_B_2-IP.

2. Attach the new shelves to the existing MetroCluster FC nodes, using FC-to-SAS bridges, if necessary.

See the requirements and procedures in [Hot-adding storage to a MetroCluster FC configuration](#)

Migrate root aggregates and move data to the new disk shelves

You must move the root aggregates from the old drive shelves to the new drive shelves that will be used by the MetroCluster IP nodes.

About this task

This task is performed prior to the transition on the existing nodes (node_A_1-FC and node_B_1-FC).

Steps

1. Perform a negotiated switchover from controller node_B_1-FC:

```
metrocluster switchover
```

2. Perform the heal aggregates and heal root steps of the recovery from node_B_1-FC:

```
metrocluster heal -phase aggregates
```

```
metrocluster heal -phase root-aggregates
```

3. Boot controller node_A_1-FC:

```
boot_ontap
```

4. Assign the unowned disks on the new shelves to the appropriate pools for controller node_A_1-FC:

a. Identify the disks on the shelves:

```
disk show -shelf pool_0_shelf -fields container-type,diskpathnames
```

```
disk show -shelf pool_1_shelf -fields container-type,diskpathnames
```

b. Enter local mode so the commands are run on the local node:

```
run local
```

c. Assign the disks:

```
disk assign disk1disk2disk3disk... -p 0
```

```
disk assign disk4disk5disk6disk... -p 1
```

d. Exit local mode:

```
exit
```

5. Create a new mirrored aggregate to become the new root aggregate for controller node_A_1-FC:

a. Set the privilege mode to advanced:

```
set priv advanced
```

b. Create the aggregate:

```
aggregate create -aggregate new_aggr -disklist disk1, disk2, disk3,... -mirror
-disklist disk4disk5, disk6,... -raidtypesame-as-existing-root -force-small
-aggregate true aggr show -aggregate new_aggr -fields percent-snapshot-space
```

If the percent-snapshot-space value is less than 5 percent, you must increase it to a value higher than 5 percent:

```
aggr modify new_aggr -percent-snapshot-space 5
```

c. Set the privilege mode back to admin:

```
set priv admin
```

6. Confirm that the new aggregate is created properly:

```
node run -node local sysconfig -r
```

7. Create the node and cluster-level configuration backups:



When the backups are created during switchover, the cluster is aware of the switched over state on recovery. You must ensure that the backup and upload of the system configuration is successful as without this backup it is **not** possible to reform the MetroCluster configuration between clusters.

a. Create the cluster backup:

```
system configuration backup create -node local -backup-type cluster -backup -name cluster-backup-name
```

b. Check cluster backup creation

```
job show -id job-idstatus
```

c. Create the node backup:

```
system configuration backup create -node local -backup-type node -backup -name node-backup-name
```

d. Check for both cluster and node backups:

```
system configuration backup show
```

You can repeat the command until both backups are shown in the output.

8. Make copies of the backups.

The backups must be stored at a separate location because they will be lost locally when the new root volume is booted.

You can upload the backups to an FTP or HTTP server, or copy the backups using `scp` commands.

Process	Steps
Upload the backup to the FTP or HTTP server	<p>a. Upload the cluster backup:</p> <pre>system configuration backup upload -node local -backup <i>cluster-backup-name</i> -destination URL</pre> <p>b. Upload the node backup:</p> <pre>system configuration backup upload -node local -backup <i>node-backup-name</i> -destination URL</pre>

Copy the backups onto a remote server using secure copy	<p>From the remote server use the following scp commands:</p> <ol style="list-style-type: none"> Copy the cluster backup: <pre>scp diagnode-mgmt-FC:/mroot/etc/backups/config/cluster-backup-name.7z .</pre> <ol style="list-style-type: none"> Copy the node backup: <pre>scp diag@node-mgmt-FC:/mroot/etc/backups/config/node-backup-name.7z .</pre>
--	--

9. Halt node_A_1-FC:

```
halt -node local -ignore-quorum-warnings true
```

10. Boot node_A_1-FC to Maintenance mode:

```
boot_ontap maint
```

11. From Maintenance mode, make required changes to set the aggregate as root:

a. Set the HA policy to cfo:

```
aggr options new_aggr ha_policy cfo
```

Respond “yes” when prompted to proceed.

Are you sure you want to proceed (y/n) ?

b. Set the new aggregate as root:

```
aggr options new_aggr root
```

c. Halt to the LOADER prompt:

```
halt
```

12. Boot the controller and back up the system configuration.

The node boots in recovery mode when the new root volume is detected

a. Boot the controller:

```
boot_ontap
```

b. Log in and back up the configuration.

When you log in, you will see the following warning:

Warning: The correct cluster system configuration backup must be restored. If a backup from another cluster or another system state is used then the root volume will need to be recreated and NGS engaged for recovery assistance.

c. Enter advanced privilege mode:

```
set -privilege advanced
```

d. Back up the cluster configuration to a server:

```
system configuration backup download -node local -source URL of server/cluster-backup-name.7z
```

e. Back up the node configuration to a server:

```
system configuration backup download -node local -source URL of server/node-backup-name.7z
```

f. Return to admin mode:

```
set -privilege admin
```

13. Check the health of the cluster:

a. Issue the following command:

```
cluster show
```

b. Set the privilege mode to advanced:

```
set -privilege advanced
```

c. Verify the cluster configuration details:

```
cluster ring show
```

d. Return to the admin privilege level:

```
set -privilege admin
```

14. 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
```

15. Perform a switchback from controller node_B_1-FC:

```
metrocluster switchback
```

16. 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
```

17. Add the new root volume to the Volume Location Database.

a. Set the privilege mode to advanced:

```
set -privilege advanced
```

b. Add the volume to the node:

```
volume add-other-volumes -node node_A_1-FC
```

c. Return to the admin privilege level:

```
set -privilege admin
```

18. Check that the volume is now visible and has mroot.

a. Display the aggregates:

```
storage aggregate show
```

b. Verify that the root volume has mroot:

```
storage aggregate show -fields has-mroot
```

c. Display the volumes:

```
volume show
```

19. Create a new security certificate to re-enable access to System Manager:

```
security certificate create -common-name name -type server -size 2048
```

20. Repeat the previous steps to migrate the aggregates on shelves owned by node_A_1-FC.

21. Perform a cleanup.

You must perform the following steps on both node_A_1-FC and node_B_1-FC to remove the old root volume and root aggregate.

a. Delete the old root volume:

```
run local

vol offline old_vo10

vol destroy old_vo10

exit

volume remove-other-volume -vserver node_name -volume old_vo10
```

b. Delete the original root aggregate:

```
aggr offline -aggregate old_aggr0_site

aggr delete -aggregate old_aggr0_site
```

22. Migrate the data volumes to aggregates on the new controllers, one volume at a time.

Refer to [Creating an aggregate and moving volumes to the new nodes](#)

23. Retire the old shelves by performing all the steps in [Retiring shelves moved from node_A_1-FC and node_A_2-FC](#).

Transitioning the configuration

You must follow the detailed transition procedure.

About this task

In the following steps you are directed to other topics. You must perform the steps in each topic in the order given.

Steps

1. Plan port mapping.

Perform all the steps in [Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes](#).

2. Prepare the MetroCluster IP controllers.

Perform all the steps in [Preparing the MetroCluster IP controllers](#).

3. Verify the health of the MetroCluster configuration.

Perform all the steps in [Verifying the health of the MetroCluster FC configuration](#).

4. Prepare and remove the existing MetroCluster FC nodes.

Perform all the steps in [Transitioning the MetroCluster FC nodes](#).

5. Add the new MetroCluster IP nodes.

Perform all the steps in [Connecting the MetroCluster IP controller modules](#).

6. Complete the transition and initial configuration of the new MetroCluster IP nodes.

Perform all the steps in [Configuring the new nodes and completing transition](#).

Moving an FC SAN workload from MetroCluster FC to MetroCluster IP nodes

When non-disruptively transitioning from MetroCluster FC to IP nodes, you must non-disruptively move FC SAN host objects from MetroCluster FC to IP nodes.

Move an FC SAN workload from MetroCluster FC to MetroCluster IP nodes

Steps

1. Set up new FC interfaces (LIFS) on MetroCluster IP nodes:

a. If required, on MetroCluster IP nodes, modify FC ports to be used for client connectivity to FC target personality.

This might require a reboot of the nodes.

b. Create FC LIFS/interfaces on IP nodes for all SAN SVMs. Optionally, verify that the WWPNs from newly created FC LIFs are logged into the FC SAN switch

2. Update SAN zoning configuration for newly added FC LIFs on MetroCluster IP nodes.

To facilitate moving of volumes that contain LUNs actively serving data to FC SAN clients, update existing FC switch zones to allow FC SAN clients to access to LUNs on MetroCluster IP nodes.

a. On the FC SAN switch (Cisco or Brocade), add the WWPNs of newly added FC SAN LIFs to the zone.

b. Update, save and commit the zoning changes.

c. From the client, check for FC initiator logins to the new SAN LIFs on the MetroCluster IP nodes:
`sanlun lun show -p`

At this time, the client should see and be logged in to the FC interfaces on both the MetroCluster FC and MetroCluster IP nodes. LUNs and volumes are still physically hosted on the MetroCluster FC nodes.

Because LUNs are reported only on MetroCluster FC node interfaces, the client shows only paths over FC nodes. This can be seen in the output of the `sanlun lun show -p` and `multipath -ll -d` commands.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
LUN: 4
LUN Size: 2g
Product: cDOT
Host Device: 3600a098038304646513f4f674e52774b
Multipath Policy: service-time 0
Multipath Provider: Native
-----
-----
host vserver
path path /dev/ host vserver
state type node adapter LIF
-----
-----
up primary sdk host3 iscsi_lf_n2_p1_
up secondary sdh host2 iscsi_lf_n1_p1_

[root@stemgr]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|--- policy='service-time 0' prio=50 status=active
|   `-- 3:0:0:4 sdk 8:160 active ready running
`--- policy='service-time 0' prio=10 status=enabled
   `-- 2:0:0:4 sdh 8:112 active ready running
```

3. Modify the reporting nodes to add the MetroCluster IP nodes

- a. List reporting nodes for LUNs on the SVM: lun mapping show -vserver svm-name -fields reporting-nodes -ostype linux

Reporting nodes shown are local nodes as LUNs are physically on FC nodes A_1 and A_2.

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver    path                      igrpup      reporting-nodes
-----  -----
vsa_1      /vol/vsa_1_voll/lun_linux_2  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_voll/lun_linux_3  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol2/lun_linux_4  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol3/lun_linux_7  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol4/lun_linux_8  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol4/lun_linux_9  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol6/lun_linux_12  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol6/lun_linux_13  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol7/lun_linux_14  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol8/lun_linux_17  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol9/lun_linux_18  igrup_linux  A_1,A_2
vsa_1      /vol/vsa_1_vol9/lun_linux_19  igrup_linux  A_1,A_2
12 entries were displayed.
```

b. Add reporting nodes to include MetroCluster IP nodes.

```
cluster_A::> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_voll*/lun_linux_* -nodes B_1,B_2 -igrpup igrup_linux

12 entries were acted on.
```

c. List reporting nodes and verify the presence of the new nodes:

```

cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path                                igrup      reporting-nodes
-----  -----
-----  -----
-----  -----
vsa_1  /vol/vsa_1_vol1/lun_linux_2  igrup_linux  A_1,A_2,B_1,B_2
vsa_1  /vol/vsa_1_vol1/lun_linux_3  igrup_linux  A_1,A_2,B_1,B_2
vsa_1  /vol/vsa_1_vol2/lun_linux_4  igrup_linux  A_1,A_2,B_1,B_2
vsa_1  /vol/vsa_1_vol3/lun_linux_7  igrup_linux  A_1,A_2,B_1,B_2
...
12 entries were displayed.

```

- d. Verify that the `sg3-utils` package is installed on the Linux host. This avoids a `rescan-scsi-bus.sh` utility not found error when you rescan the Linux host for the newly mapped LUNs using the `rescan-scsi-bus` command.
- e. Rescan the SCSI bus on the host to discover the newly added paths: `/usr/bin/rescan-scsi-bus.sh -a`

```

[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning for device 2 0 0 0 ...
.
.
.

OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
  Vendor: NETAPP Model: LUN C-Mode Rev: 9800
  Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.

```

- f. Display the newly added paths: `sanlun lun show -p`

Each LUN will have four paths.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
LUN: 4
LUN Size: 2g
Product: CDOT
Host Device: 3600a098038304646513f4f674e52774b
Multipath Policy: service-time 0
Multipath Provider: Native
-----
-----
host vserver
path path /dev/ host vserver
state type node adapter LIF
-----
-----
up primary sdk host3 iscsi_lf_n2_p1_
up secondary sdh host2 iscsi_lf_n1_p1_
up secondary sdag host4 iscsi_lf_n4_p1_
up secondary sdah host5 iscsi_lf_n3_p1_
```

g. On the controllers, move the volumes containing LUNs from the MetroCluster FC to the MetroCluster IP nodes.

```
cluster_A::> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate A_1_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "A_1_htp_005_aggr1". Use the "volume move show -vserver
vsa_1 -volume vsa_1_vol1"
command to view the status of this operation.
cluster_A::> volume move show
Vserver      Volume      State      Move Phase      Percent-Complete Time-To-
Complete
-----
-----
vsa_1      vsa_1_vol1  healthy    initializing
--
```

h. On the FC SAN client, display the LUN information: `sanlun lun show -p`

The FC interfaces on the MetroCluster IP nodes where the LUN now resides are updated as primary paths. If the primary path is not updated after the volume move, run `/usr/bin/rescan-scsi-bus.sh -a` or simply wait for multipath rescanning to take place.

The primary path in the following example is the LIF on MetroCluster IP node.

```
[root@localhost ~]# sanlun lun show -p

        ONTAP Path: vsa_1:/vol/vsa_1_voll/lun_linux_2
                      LUN: 22
                      LUN Size: 2g
                      Product: cDOT
                      Host Device: 3600a098038302d324e5d50305063546e
                      Multipath Policy: service-time 0
                      Multipath Provider: Native
-----
-----
host      vserver
path      path      /dev/    host      vserver
state     type      node     adapter   LIF
-----
-----
up        primary    sddv     host6    fc_5
up        primary    sdjx     host7    fc_6
up        secondary  sdgv     host6    fc_8
up        secondary  sdkr     host7    fc_8
```

- Repeat the above steps for all volumes, LUNs and FC interfaces belonging to a FC SAN host.

When completed, all LUNs for a given SVM and FC SAN host should be on MetroCluster IP nodes.

- Remove the reporting nodes and re-scan paths from client.

- Remove the remote reporting nodes (the MetroCluster FC nodes) for the linux LUNs: lun mapping remove-reporting-nodes -vserver vsa_1 -path * -igroup igrup_linux -remote-nodes true

```
cluster_A::> lun mapping remove-reporting-nodes -vserver vsa_1 -path
* -igroup igrup_linux -remote-nodes true
12 entries were acted on.
```

- Check reporting nodes for the LUNs: lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux

```

cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igrup reporting-nodes
-----
-----
vsa_1 /vol/vsa_1_voll/lun_linux_2 igrup_linux B_1,B_2
vsa_1 /vol/vsa_1_voll/lun_linux_3 igrup_linux B_1,B_2
vsa_1 /vol/vsa_1_voll/lun_linux_4 igrup_linux B_1,B_2
...
12 entries were displayed.

```

c. Rescan the SCSI bus on the client: /usr/bin/rescan-scsi-bus.sh -r

The paths from the MetroCluster FC nodes are removed:

```

[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
    Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
    Vendor: NETAPP Model: LUN C-Mode Rev: 9800
    Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
[2:0:0:0]
[2:0:0:1]
...

```

d. Verify that only paths from the MetroCluster IP nodes are visible from the host: sanlun lun show -p

- e. If required, remove iSCSI LIFs from the MetroCluster FC nodes.

This should be done if there are no other LUNs on the nodes mapped to other clients.

Move Linux iSCSI hosts from MetroCluster FC to MetroCluster IP nodes

After you transition your MetroCluster nodes from FC to IP, you might need to move your iSCSI host connections to the new nodes.

About this task

- IPv4 interfaces are created when you set up the new iSCSI connections.
- The host commands and examples are specific to Linux operating systems.
- The MetroCluster FC nodes are called old nodes and the MetroCluster IP nodes are called new nodes.

Step 1: Set up new iSCSI connections

To move the iSCSI connections, you set up new iSCSI connections to the new nodes.

Steps

1. Create iSCSI interfaces on the new nodes and check ping connectivity from the iSCSI hosts to the new interfaces on the new nodes.

[Create network interfaces](#)

All iSCSI interfaces from the SVM should be reachable by the iSCSI host.

2. On the iSCSI host, identify the existing iSCSI connections from the host to the old node:

```
iscsiadm -m session
```

```
[root@scspr1789621001 ~]# iscsiadm -m session
tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

3. On the new node, verify the connections from the new node:

```
iscsi session show -vserver <svm-name>
```

```
node_A_1-new::*> iscsi session show -vserver vsa_1
  Tpgroup Initiator Initiator
  Vserver Name TSIH Name ISID Alias
  -----
  -----
  vsa_1 iscsi_lf_n1_p1_ 4 iqn.2020-
  01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01
  scspr1789621001.gdl.englab.netapp.com
  vsa_1 iscsi_lf_n2_p1_ 4 iqn.2020-
  01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02
  scspr1789621001.gdl.englab.netapp.com
  2 entries were displayed.
```

4. On the new node, list the iSCSI interfaces in ONTAP for the SVM that contains the interfaces:

```
iscsi interface show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi interface show -vserver vsa_1
  Logical Status Curr Curr
  Vserver Interface TPGT Admin/Oper IP Address Node Port Enabled
  -----
  -----
  vsa_1 iscsi_lf_n1_p1_ 1156 up/up 10.230.68.236 sti8200mcc-htp-001 e0g
  true
  vsa_1 iscsi_lf_n1_p2_ 1157 up/up fd20:8b1e:b255:805e::78c9 sti8200mcc-
  htp-001 e0h true
  vsa_1 iscsi_lf_n2_p1_ 1158 up/up 10.230.68.237 sti8200mcc-htp-002 e0g
  true
  vsa_1 iscsi_lf_n2_p2_ 1159 up/up fd20:8b1e:b255:805e::78ca sti8200mcc-
  htp-002 e0h true
  vsa_1 iscsi_lf_n3_p1_ 1183 up/up 10.226.43.134 sti8200mccip-htp-005 e0c
  true
  vsa_1 iscsi_lf_n4_p1_ 1188 up/up 10.226.43.142 sti8200mccip-htp-006 e0c
  true
  6 entries were displayed.
```

5. On the iSCSI host, run discovery on any one of the iSCSI IP addresses on the SVM to discover the new targets:

```
iscsiadm -m discovery -t sendtargets -p iscsi-ip-address
```

Discovery can be run on any IP address of the SVM, including non-iSCSI interfaces.

```
[root@scspr1789621001 ~]# iscsiadadm -m discovery -t sendtargets -p  
10.230.68.236:3260  
10.230.68.236:3260,1156 iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6  
10.226.43.142:3260,1188 iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6  
10.226.43.134:3260,1183 iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6  
10.230.68.237:3260,1158 iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
```

6. On the iSCSI host, login to all the discovered addresses:

```
iscsiadm -m node -L all -T node-address -p portal-address -l
```

```
[root@scspr1789621001 ~]# iscsiadadm -m node -L all -T iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 -p  
10.230.68.236:3260 -l  
Logging in to [iface: default, target: iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:  
10.226.43.142,3260] (multiple)  
Logging in to [iface: default, target: iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:  
10.226.43.134,3260] (multiple)  
Login to [iface: default, target: iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:  
10.226.43.142,3260] successful.  
Login to [iface: default, target: iqn.1992-  
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:  
10.226.43.134,3260] successful.
```

7. On the iSCSI host, verify the login and connections:

```
iscsiadm -m session
```

```
[root@scspr1789621001 ~]# iscsiadm -m session
tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [3] 10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

8. On the new node, verify the login and connection with the host:

```
iscsi initiator show -vserver <svm-name>
```

```
sti8200mcchtp001http_siteA::*> iscsi initiator show -vserver vsa_1
Tpgroup Initiator
Vserver Name          TSIH Name          ISID
Igroup Name
----- ----- -----
----- -----
vsa_1 iscsi_lf_n1_p1_ 4 iqn.2020-
01.com.netapp.englabsdl:scspr1789621001 00:02:3d:00:00:01 igroup_linux
vsa_1 iscsi_lf_n2_p1_ 4 iqn.2020-
01.com.netapp.englabsdl:scspr1789621001 00:02:3d:00:00:02 igroup_linux
vsa_1 iscsi_lf_n3_p1_ 1 iqn.2020-
01.com.netapp.englabsdl:scspr1789621001 00:02:3d:00:00:04 igroup_linux
vsa_1 iscsi_lf_n4_p1_ 1 iqn.2020-
01.com.netapp.englabsdl:scspr1789621001 00:02:3d:00:00:03 igroup_linux
4 entries were displayed.
```

Result

At the end of this task, the host can see all iSCSI interfaces (on the old and new nodes) and is logged in to all those interfaces.

LUNs and volumes are still physically hosted on the old nodes. Because LUNs are reported only on the old node interfaces, the host will show only paths over the old nodes. To see this, run the `sanlun lun show -p` and `multipath -ll -d` commands on the host and examine the command outputs.

```
[root@scspr1789621001 ~]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
LUN: 4
LUN Size: 2g
Product: cDOT
Host Device: 3600a098038304646513f4f674e52774b
Multipath Policy: service-time 0
Multipath Provider: Native
-----
host vserver
path path /dev/ host vserver
state type node adapter LIF
-----
up primary sdk host3 iscsi_lf_n2_p1_
up secondary sdh host2 iscsi_lf_n1_p1_
[root@scspr1789621001 ~]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|--- policy='service-time 0' prio=50 status=active
| `-- 3:0:0:4 sdk 8:160 active ready running
`-- policy='service-time 0' prio=10 status=enabled
`- 2:0:0:4 sdh 8:112 active ready running
```

Step 2: Add the new nodes as reporting nodes

After setting up the connections to the new nodes, you add the new nodes as the reporting nodes.

Steps

1. On the new node, list reporting nodes for LUNs on the SVM:

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux
```

The following reporting nodes are local nodes as LUNs are physically on old nodes node_A_1-old and node_A_2-old.

```

node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver path                      igrup      reporting-nodes
-----
-----
vsa_1    /vol/vsa_1_voll/lun_linux_2  igrup_linux node_A_1-old,node_A_2-
old
.
.
.
vsa_1    /vol/vsa_1_vol9/lun_linux_19  igrup_linux node_A_1-old,node_A_2-
old
12 entries were displayed.

```

2. On the new node, add reporting nodes:

```

lun mapping add-reporting-nodes -vserver <svm-name> -path
/vol/vsa_1_vol*/lun_linux_* -nodes node1,node2 -igroup <igroup_name>

```

```

node_A_1-new::*> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes node_A_1-new,node_A_2-new
-igroup igrup_linux
12 entries were acted on.

```

3. On the new node, verify that the newly added nodes are present:

```

lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux vserver path igrup reporting-nodes

```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux vserver path igrup reporting-nodes
-----
-----
-----
vsa_1 /vol/vsa_1_voll/lun_linux_2 igrup_linux node_A_1-old, node_A_2-
old, node_A_1-new, node_A_2-new
vsa_1 /vol/vsa_1_voll/lun_linux_3 igrup_linux node_A_1-old, node_A_2-
old, node_A_1-new, node_A_2-new
.
.
.
12 entries were displayed.
```

4. The `sg3-utils` package must be installed on the Linux host. This prevents a `rescan-scsi-bus.sh` utility not found error when you rescan the Linux host for the newly mapped LUNs using the `rescan-scsi-bus` command.

On the host, verify that the `sg3-utils` package is installed:

- For a Debian based distribution:

```
dpkg -l | grep sg3-utils
```

- For a Red Hat based distribution:

```
rpm -qa | grep sg3-utils
```

If required, install the `sg3-utils` package on the Linux host:

```
sudo apt-get install sg3-utils
```

5. On the host, rescan the SCSI bus on the host and discover the newly added paths:

```
/usr/bin/rescan-scsi-bus.sh -a
```

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
  Vendor: NETAPP Model: LUN C-Mode Rev: 9800
  Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

6. On the iSCSI host, list the newly added paths:

```
sanlun lun show -p
```

Four paths are shown for each LUN.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
  LUN: 4
  LUN Size: 2g
  Product: cDOT
  Host Device: 3600a098038304646513f4f674e52774b
  Multipath Policy: service-time 0
  Multipath Provider: Native
  -----
  host vserver
  path path /dev/ host vserver
  state type      node    adapter      LIF
  -----
  up    primary    sdk     host3      iscsi_lf_n2_p1_
  up    secondary  sdh     host2      iscsi_lf_n1_p1_
  up    secondary  sdag    host4      iscsi_lf_n4_p1_
  up    secondary  sdah    host5      iscsi_lf_n3_p1_
```

7. On the new node, move the volume/volumes containing LUNs from the old nodes to the new nodes.

```

node_A_1-new::*> vol move start -vserver vsa_1 -volume vsa_1_voll
-destination-aggregate sti8200mccip_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_voll" in Vserver "vsa_1" to
aggregate "sti8200mccip_htp_005_aggr1". Use the "volume move show
-vserver
vsa_1 -volume vsa_1_voll" command to view the status of this operation.
node_A_1-new::*> vol move show
Vserver  Volume      State      Move      Phase      Percent-
Complete  Time-To-Complete
-----
-----
vsa_1    vsa_1_voll  healthy    initializing  -
-
```

- When the volume move to the new nodes is complete, verify that the volume is online:

```
volume show -state
```

- The iSCSI interfaces on the new nodes where the LUN now resides are updated as primary paths. If the primary path is not updated after the volume move, run `/usr/bin/rescan-scsi-bus.sh -a` and `multipath -v3` on the host or simply wait for multipath rescanning to take place.

In the following example, the primary path is a LIF on the new node.

```

[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_voll/lun_linux_12
LUN: 4
LUN Size: 2g
Product: cDOT
Host Device: 3600a098038304646513f4f674e52774b
Multipath Policy: service-time 0
Multipath Provider: Native
-----
host vserver
path path /dev/ host vserver
state  type      node    adapter      LIF
-----
up    primary    sdag    host4      iscsi_lf_n4_p1_
up    secondary  sdk     host3      iscsi_lf_n2_p1_
up    secondary  sdh     host2      iscsi_lf_n1_p1_
up    secondary  sdah    host5      iscsi_lf_n3_p1_
```

Step 3: Remove reporting nodes and rescan paths

You must remove the reporting nodes and rescan the paths.

Steps

1. On the new node, remove remote reporting nodes (the new nodes) for the Linux LUNs:

```
lun mapping remove-reporting-nodes -vserver <svm-name> -path * -igroup
<igroup_name> -remote-nodes true
```

In this case, the remote nodes are old nodes.

```
node_A_1-new::*> lun mapping remove-reporting-nodes -vserver vsa_1 -path
* -igroup igroup_linux -remote-nodes true
12 entries were acted on.
```

2. On the new node, check reporting nodes for the LUNs:

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver    path                  igrup      reporting-nodes
-----  -----
-----  -----
vsa_1      /vol/vsa_1_voll/lun_linux_2  igrup_linux  node_A_1-
new, node_A_2-new
vsa_1      /vol/vsa_1_voll/lun_linux_3  igrup_linux  node_A_1-
new, node_A_2-new
vsa_1      /vol/vsa_1_vol2/lun_linux_4  igrup_linux  node_A_1-
new, node_A_2-new
.
.
.
12 entries were displayed.
```

3. The `sg3-utils` package must be installed on the Linux host. This prevents a `rescan-scsi-bus.sh` utility not found error when you rescan the Linux host for the newly mapped LUNs using the `rescan-scsi-bus` command.

On the host, verify that the `sg3-utils` package is installed:

- For a Debian based distribution:

```
dpkg -l | grep sg3-utils
```

- For a Red Hat based distribution:

```
rpm -qa | grep sg3-utils
```

If required, install the `sg3-utils` package on the Linux host:

```
sudo apt-get install sg3-utils
```

4. On the iSCSI host, rescan the SCSI bus:

```
/usr/bin/rescan-scsi-bus.sh -r
```

The paths that are removed are the paths from the old nodes.

```
[root@scspr1789621001 ~]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)

.
.

.

OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
Vendor: NETAPP Model: LUN C-Mode Rev: 9800
Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
[2:0:0:0]
[2:0:0:1]
.
```

5. On the iSCSI host, verify that only paths from the new nodes are visible:

```
sanlun lun show -p
```

```
multipath -ll -d
```

Where to find additional information

You can learn more about MetroCluster configuration.

MetroCluster and miscellaneous information

Information	Subject
-------------	---------

MetroCluster IP Solution Architecture and Design, TR-4689	<ul style="list-style-type: none"> • A technical overview of the MetroCluster IP configuration and operation. • Best practices for a MetroCluster IP configuration.
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	<ul style="list-style-type: none"> • Understanding the MetroCluster configuration • Switchover, healing, and switchback
Disaster Recovery	<ul style="list-style-type: none"> • Disaster recovery • Forced switchover • Recovery from a multi-controller or storage failure
MetroCluster Maintenance	<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 and Expansion	<ul style="list-style-type: none"> Upgrading or refreshing a MetroCluster configuration Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Transition	<ul style="list-style-type: none"> Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration
MetroCluster Upgrade, Transition, and Expansion	<ul style="list-style-type: none"> Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software
ONTAP Hardware Systems Documentation	<ul style="list-style-type: none"> Hot-adding a disk shelf Hot-removing a disk shelf
Note: The standard storage shelf maintenance procedures can be used with MetroCluster IP configurations.	
Copy-based transition	<ul style="list-style-type: none"> Transitioning data from 7-Mode storage systems to clustered storage systems
ONTAP concepts	<ul style="list-style-type: none"> How mirrored aggregates work

Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.