Connecting the MetroCluster IP controller modules

ONTAP MetroCluster

aherbin, Amanda Stroman, netapp-martyh, netapp-thomi, ntap-bmegan, zachary wambold

April 30, 2021

Table of Contents

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.

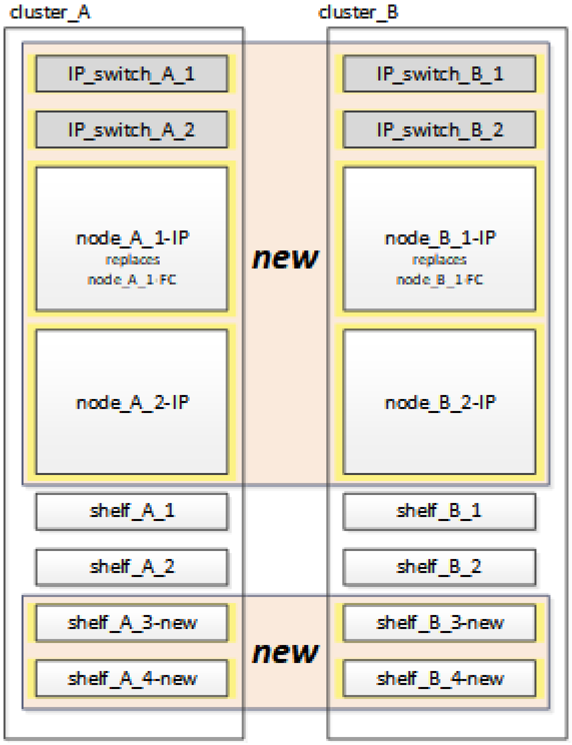
Setting up the new controllers

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

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.



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.

   AFF and FAS Documentation Center

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

   MetroCluster IP installation and configuration

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

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

    MetroCluster IP installation and configuration

    - Resetting the Broadcom IP switch to factory defaults
    - Resetting the Cisco IP switch to factory defaults
11. Download and install the RCF files.

    Follow the steps in the section for your switch vendor from the MetroCluster IP installation and configuration.

    - Downloading and installing the Broadcom RCF files
    - Downloading and installing the Cisco IP RCF files
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.

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 reassignments 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. **Note:**
    - 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	security key-manager onboard sync For more information, see Restoring onboard key management encryption keys.
External key management	security key-manager key query -node node-name For more information, see Restoring external key management encryption keys. +

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.

You must have the passphrases gathered earlier.

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 enter 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-addresssetenv bootarg.kmip.init.netmask netmasksetenv 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-addresssetenv bootarg.kmip.init.netmask netmasksetenv 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.

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.

NOTE:

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

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`

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.

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 lifname -vserver vservername -home-port new-datahomeport`
   c. If the LIF is not a data LIF: `network interface modify -lif lifname -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 a1name -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 a1name -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.

1. Verify if the management LIF and cluster management LIFs are on 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 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 using `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 using the following commands:

   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 -lifintercluster-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

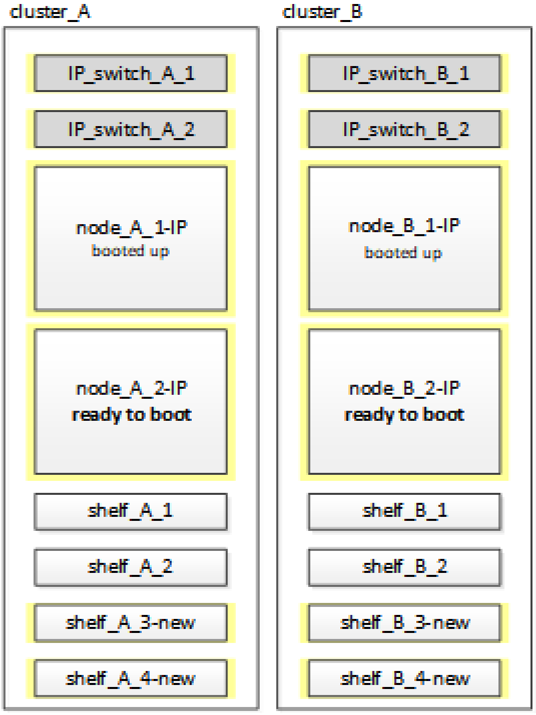
You must boot the new controller modules one at a time using the correct option at the boot menu.

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



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
                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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	security key-manager onboard sync For more information, see Restoring onboard key management encryption keys.
External key management	security key-manager key query -node node-name For more information, see Restoring external key management encryption keys. +

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 using the following commands

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.

1. Configure the intercluster LIFs using the procedures in the *MetroCluster IP Installation and Configuration Guide*.

   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.

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
           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
```

2. Ping to check that the peer addresses are reachable: `cluster peer ping -originating-node local-node -destination-cluster remote-cluster-name`

Copyright Information

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

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

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

Trademark Information