## Contents

Deciding whether to use this guide ................................................................. 7
Where to find procedures for MetroCluster expansion and maintenance tasks .................................................................................... 8

### Performing FC-to-SAS bridge maintenance .................................................. 11
- Support for FibreBridge 7600N bridges in MetroCluster configurations .......... 11
- Support for FibreBridge 7500N bridges in MetroCluster configurations .......... 12
- Enabling IP port access on the FibreBridge 7600N bridge if necessary .......... 13
- Updating firmware on a FibreBridge bridge ...................................................... 14
  - Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later ................................................. 14
  - Updating firmware on FibreBridge 7500N on configurations running ONTAP 9.3.x and earlier or 6500N bridges ..................................................... 17
- Replacing a single FC-to-SAS bridge ............................................................... 20
  - Verifying storage connectivity ................................................................. 20
  - Hot-swapping a bridge with a replacement bridge of the same model ....... 21
  - Hot-swapping a FibreBridge 7500N with a 7600N bridge ......................... 27
  - Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge ................................................................................. 33
- Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges ..... 39
  - Verifying storage connectivity ................................................................. 40
  - Hot-swapping FibreBridge 6500N bridges to create a pair of FibreBridge 7600N or 7500N bridges ................................................................. 41
- Cabling the bridge SAS ports when consolidating storage behind FibreBridge 7600N or 7500N bridges ................................................................. 46
  - Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration ................................................................. 50
  - Cabling the second bridge FC port when adding FibreBridge 7600N or 7500N bridges to a configuration ................................................................. 54
  - Disabling unused SAS ports on the FC-to-SAS bridges ............................... 57
- Requirements for using other interfaces to configure and manage FibreBridge bridges ................................................................. 58
- Hot-replacing a failed power supply module ................................................. 59
- In-band management of the FC-to-SAS bridges ............................................. 59
  - Managing a FibreBridge bridge from ONTAP ............................................. 60
  - Securing or unsecuring the FibreBridge bridge ........................................... 60

### Performing FC switch maintenance and replacement ............................... 62
- Upgrading or downgrading the firmware on a Brocade FC switch ................. 62
- Upgrading or downgrading the firmware on a Cisco FC switch .................... 65
- Upgrading to new Brocade FC switches ....................................................... 67
- Replacing a Brocade FC switch ................................................................. 71
- Renaming a Brocade FC switch ................................................................. 75
Changing ISL properties, ISL ports, or the IOD/OOD configuration on a Brocade switch .................................................................................................... 77
Replacing a Cisco FC switch ........................................................................... 81
Changing speed of ISL ports on a Cisco FC switch ........................................... 88
Adding ISLs to a Cisco switch ............................................................................. 89

Performing IP switch maintenance and replacement ................................. 91
Renaming a Cisco IP switch ............................................................................. 91
Changing ISL port speed or adding ISL ports on a Cisco IP switch .... 93
Identifying storage in a MetroCluster IP configuration ............................. 95
Hot-adding storage to a MetroCluster FC configuration .......................... 97
Hot-adding a SAS disk shelf in a direct-attached MetroCluster FC configuration using SAS optical cables ................................................................. 97
Hot-adding SAS storage to a bridge-attached MetroCluster FC configuration .... 97
Hot-adding a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges ................................................................. 98
Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system ................................................................. 104
Hot-adding a SAS disk shelf to a stack of SAS disk shelves ..................... 115

Hot-removing storage from a MetroCluster FC configuration ............. 120
Replacing a shelf nondisruptively in a fabric-attached MetroCluster configuration ........................................................................................................ 123
Disabling access to the shelf .......................................................................... 123
Replacing the shelf ......................................................................................... 126
Reenabling access and verifying the operation ................................................ 126

When to migrate root volumes to a new destination ............................ 128
Moving a metadata volume in MetroCluster configurations ..................... 129
Renaming a cluster in MetroCluster configurations ................................... 131
Powering off and powering on a data center .............................................. 133
Powering off a MetroCluster site ................................................................. 133
Relocating the powered-off site of the MetroCluster ................................... 137
Reestablishing the MetroCluster configuration and returning to normal operation ......................................................................................... 140

Expanding a two-node MetroCluster FC configuration to a four-node configuration ......................................................................................... 143
Verifying the state of the MetroCluster configuration ................................. 145
Sending a custom AutoSupport message before adding nodes to the MetroCluster configuration ................................................................. 147
Zoning for the new controller ports when adding a controller module in a fabric-attached MetroCluster configuration ........................................ 147
Adding a new controller module to each cluster ......................................... 147
Preparing for the upgrade ............................................................................ 150
Preparing cluster ports on an existing controller module .......................... 151
Preparing the netboot server to download the image .................................. 153
Setting the HA mode on the existing controller module ............................. 154
Shutting down the existing controller module ............................................ 154
Installing and cabling the new controller module ........................................ 155
Powering up both controller modules and displaying the LOADER
prompt .................................................................................................... 157
Configuring and cabling CNA ports (80xx systems only) .......................... 158
Changing the ha-config setting on the existing and new controller
modules .................................................................................................. 159
Setting the partner system ID for both controller modules ......................... 160
Booting the existing controller module ....................................................... 160
Assigning disks to the new controller module ............................................ 160
Netbooting and setting up ONTAP on the new controller module .......... 161
Mirroring the root aggregate on the new controller .................................. 165
Configuring intercluster LIFs ...................................................................... 166
Creating a mirrored data aggregate on each node ....................................... 170
Installing licenses for the new controller module ...................................... 171
Creating unmirrored data aggregates .......................................................... 171
Installing the firmware after adding a controller module ......................... 173
Refreshing the MetroCluster configuration with new controllers ............. 173
Enabling storage failover on both controller modules and enabling cluster HA ... 175
Restarting the SVMs ............................................................................................... 175

Expanding a four-node MetroCluster FC configuration to an eight-
node configuration ........................................................................... 177

Determining the new cabling layout ......................................................... 179
Racking the new equipment ................................................................. 179
Verifying the health of the MetroCluster configuration .......................... 179
Checking for MetroCluster configuration errors with Config Advisor .......... 181
Sending a custom AutoSupport message prior to adding nodes to the
MetroCluster configuration ........................................................................ 181
Recabling and zoning a switch fabric for the new nodes ......................... 182
Disconnecting the existing DR group from the fabric ............................ 182
Applying the RCF files and recabling the switches ................................. 182

Configuring ONTAP on the new controllers ............................................... 183
Restoring system defaults and configuring the HBA type on a previously
used controller module ............................................................................ 184
Assigning disk ownership in AFF systems .............................................. 185
Assigning disk ownership in non-AFF systems ....................................... 187
Verifying the ha-config state of components ............................................ 189
Booting the new controllers and joining them to the cluster .................... 189
Configuring the clusters into a MetroCluster configuration .................... 191
Checking for MetroCluster configuration errors with Config Advisor .......... 203
Sending a custom AutoSupport message after to adding nodes to the
MetroCluster configuration ........................................................................ 203
Verifying switchover, healing, and switchback ....................................... 203

Reconfiguring the FC switch layout for ONTAP 9.1 or later ............... 204

Sending a custom AutoSupport message prior to reconfiguring switches .......... 204
Verifying the health of the MetroCluster configuration ................................ 205
Checking for MetroCluster configuration errors .......................................................... 206
Persistently disabling the switches ........................................................................... 206
Determining the new cabling layout ....................................................................... 207
Applying RCF files and recabling the switches ...................................................... 207
Persistently enable the switches ............................................................................. 208
Verifying switchover, healing, and switchback ..................................................... 208

**Port assignments for FC switches** ................................................................ 209
- Port assignments for systems using two initiator ports .................................... 209
- Port assignments for FC switches when using ONTAP 9.0 ............................ 210
- Port assignments for FC switches when using ONTAP 9.1 and later ............. 224

**Using the Interoperability Matrix Tool to find MetroCluster information** .......................................................... 239
**Where to find additional information** ............................................................. 240
**Copyright** ........................................................................................................ 241
**Trademark** ..................................................................................................... 242
**How to send comments about documentation and receive update notifications** ........................................................................................................ 243
Deciding whether to use the MetroCluster Service Guide

This guide describes how to perform maintenance on the MetroCluster hardware components. You should use this guide for maintaining the MetroCluster-specific hardware components in your MetroCluster configuration.

You can find other MetroCluster documentation in the following location:

ONTAP 9 Documentation Center
# Where to find procedures for MetroCluster expansion and maintenance tasks

You should be sure you select the correct procedure when you perform MetroCluster hardware expansion and maintenance tasks.

<table>
<thead>
<tr>
<th>Component</th>
<th>MetroCluster type (FC or IP)</th>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Storage controller module| FC                           | MetroCluster FC expansion (adding controller modules to expand a two-node configuration to four nodes or expand a four-node configuration to eight nodes) | *Expanding a two-node MetroCluster FC configuration to a four-node configuration on page 143*
<p>|                          |                              |                                                                     | <em>Expanding a four-node MetroCluster FC configuration to an eight-node configuration on page 177</em> |
| Both                     | ONTAP software upgrade       |                                                                     | <em>Upgrade, revert, or downgrade</em>                                          |
| Both                     | Hardware upgrade             |                                                                     | <em>AFF and FAS Documentation Center</em>                                       |
| Both                     | FRU replacement (including controller modules, PCIe cards, FC-VI card, and so on) | <strong>Note:</strong> Moving a storage controller module or NVRAM card among the MetroCluster storage systems is not supported. |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>MetroCluster type (FC or IP)</th>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Drive shelf               | FC                            | Shelf addition (stack with bridges or individual shelf)              | *Hot-adding a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges on page 98  
|                           |                               |                                                                      | *Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system on page 104  
|                           |                               |                                                                      | *Hot-adding a SAS disk shelf to a stack of SAS disk shelves on page 115  
| FC                        | Shelf removal                 |                                                                     | *Hot-removing storage from a MetroCluster FC configuration on page 120  
| FC                        | All other shelf maintenance procedures. The standard procedures can be used. | DS460C, DS224C, and DS212C Disk Shelves: Service Guide  
| IP                        | All shelf maintenance procedures. The standard procedures can be used. | DS460C, DS224C, and DS212C Disk Shelves: Service Guide  
| FC-to-SAS bridge          | FC                            | Bridge replacement                                                  | Replacing a single FC-to-SAS bridge on page 20  
|                           |                               |                                                                      | Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges on page 39  
|                           |                               |                                                                      | Hot-swapping a FibreBridge 7500N with a 7600N bridge on page 27  
| FC                        | Firmware upgrade              |                                                                     | Updating the firmware on a FibreBridge bridge on page 17  
| FC                        | Replacing a failed power supply module |                                                                     | Hot-replacing a failed power supply module on page 59  

<table>
<thead>
<tr>
<th>Component</th>
<th>MetroCluster type (FC or IP)</th>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC switch</td>
<td>FC</td>
<td>Switch upgrade</td>
<td>Upgrading to new Brocade FC switches on page 67</td>
</tr>
<tr>
<td>FC</td>
<td>Switch replacement</td>
<td>Replacing a Brocade FC switch (MetroCluster) on page 71</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Replacing a Cisco FC switch on page 81</td>
</tr>
<tr>
<td>FC</td>
<td>Firmware upgrade</td>
<td>Updating firmware on a Brocade FC switch on page 62</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating firmware on a Cisco FC switch on page 65</td>
<td></td>
</tr>
<tr>
<td>SAS optical cables</td>
<td>FC</td>
<td>Cable replacement</td>
<td>NetApp Documentation: Disk Shelves</td>
</tr>
<tr>
<td>Cluster interconnect switches</td>
<td>FC</td>
<td>Switch replacement</td>
<td>NetApp Documentation: Cluster Management and Interconnect Switches</td>
</tr>
<tr>
<td>Both</td>
<td>Firmware upgrade</td>
<td>NetApp Documentation: Cluster Management and Interconnect Switches</td>
<td></td>
</tr>
</tbody>
</table>
Performing FC-to-SAS bridge maintenance

If necessary, you can nondisruptively replace the FC-to-SAS bridges or upgrade their firmware in the MetroCluster configuration.

Choices

- Support for FibreBridge 7600N bridges in MetroCluster configurations on page 11
- Support for FibreBridge 7500N bridges in MetroCluster configurations on page 12
- Enabling IP port access on the FibreBridge 7600N bridge if necessary on page 13
- Updating firmware on a FibreBridge bridge on page 14
- Replacing a single FC-to-SAS bridge on page 20
- Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges on page 39
- Requirements for using other interfaces to configure and manage FibreBridge bridges on page 58
- Hot-replacing a failed power supply module on page 59
- In-band management of the FC-to-SAS bridges on page 59
- Securing or unsecuring the FibreBridge bridge on page 60

Support for FibreBridge 7600N bridges in MetroCluster configurations

The FibreBridge 7600N bridge is supported on ONTAP 9.5 and later as a replacement for the FibreBridge 7500N or 6500N bridge or when adding new storage to the MetroCluster configuration. The zoning requirements and restrictions regarding use of the bridge's FC ports are the same as that of the FibreBridge 7500N bridge.

NetApp Interoperability Matrix Tool

<table>
<thead>
<tr>
<th>Use case</th>
<th>Zoning changes needed?</th>
<th>Restrictions</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replacing a single FibreBridge 7500N bridge</td>
<td>No</td>
<td>The FibreBridge 7600N bridge must be configured exactly the same as the FibreBridge 7500N bridge.</td>
<td>Hot-swapping a FibreBridge 7500N with a 7600N bridge on page 27</td>
</tr>
<tr>
<td>bridge with a single FibreBridge 7600N bridge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replacing a single FibreBridge 6500N bridge</td>
<td>No</td>
<td>The FibreBridge 7600N bridge must be configured exactly the same as the FibreBridge 6500N bridge.</td>
<td>Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge on page 33</td>
</tr>
</tbody>
</table>
Use case | Zoning changes needed? | Restrictions | Procedure |
--- | --- | --- | --- |
Adding new storage through adding a new pair of FibreBridge 7600N bridges | Yes | You must have available ports on the FC switch fabric (in a fabric-attached MetroCluster configuration) or on the storage controllers (in a stretch MetroCluster configuration). Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks. | Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system on page 104 |
Replacing a single FibreBridge 6500N bridge with a single FibreBridge 7500N bridge | No | The FibreBridge 7500N bridge must be configured exactly the same as the FibreBridge 6500N bridge, using a single FC port and attaching to a single stack. The second FC port on the FibreBridge 7500N must not be used. | Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge on page 33 |
Consolidating multiple stacks by replacing multiple pairs of FibreBridge 6500N bridges with a single pair of FibreBridge 7500N bridges | Yes | In this case, you take the FibreBridge 6500N bridges out of service and replace them with a single pair of FibreBridge 7500N bridges. Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks. At the end of the procedure, both the top and bottom of the stacks must be connected to corresponding ports on the FibreBridge 7500N bridges. | Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges on page 39 |
### Use case

<table>
<thead>
<tr>
<th>Zoning changes needed?</th>
<th>Restrictions</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>You must have available ports on the FC switch fabric (in a fabric-attached MetroCluster configuration) or on the storage controllers (in a stretch MetroCluster configuration). Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks.</td>
<td><strong>Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system</strong> on page 104</td>
</tr>
<tr>
<td>You must add storage zones for each of the FC ports of the new bridges.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Enabling IP port access on the FibreBridge 7600N bridge if necessary

If you are using an ONTAP version prior to 9.5, or otherwise plan to use out-of-band access to the FibreBridge 7600N bridge using telnet or other IP port protocols and services (FTP, ExpressNAV, ICMP, or QuickNAV), you can enable the access services via the console port.

**About this task**

Unlike the ATTO FibreBridge 7500N and 6500N bridges, the FibreBridge 7600N bridge is shipped with all IP port protocols and services disabled.

Starting with ONTAP 9.5, *in-band management* of the bridges is supported. This means the bridges can be configured and monitored from the ONTAP CLI via the FC connection to the bridge. Physical access to the bridge via the bridge Ethernet ports is not required and the bridge user interfaces are not required.

This task is required if you have FibreBridge 7600N bridges and you are running ONTAP 9.5 or later and are not planning on using in-band management to manage the bridges. Therefore, you need to configure the bridge via the Ethernet management port.

**Steps**

1. Access the bridge’s console interface by connecting a serial cable to the serial port on the FibreBridge 7600N bridge.

2. Using the console, enable the access services, and then save the configuration:

   ```bash
   set closeport none
   saveconfiguration
   ```

   The `set closeport none` command enables all access services on the bridge.

3. Disable specific services, if desired, and then save the configuration:

   ```bash
   set closeport service
   saveconfiguration
   ```

   `service` can specify one of the following:

   - `expressnav`
   - `ftp`
   - `icmp`
quicknav
snmp
telnet

You can check whether a specific protocol is enabled or disabled by using the `get closeport` command.

**Updating firmware on a FibreBridge bridge**

The procedure for updating the bridge firmware depends on your bridge model and ONTAP version.

**Choices**

- **Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later** on page 14
- **Updating firmware on FibreBridge 7500N on configurations running ONTAP 9.3.x and earlier or 6500N bridges** on page 17

**Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later**

You might need to update the firmware on your FibreBridge bridges to ensure that you have the latest features or to resolve possible issues. This procedure should be used for FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later.

**Before you begin**

- The MetroCluster configuration must be operating normally.
- All of the FibreBridge bridges in the MetroCluster configuration must be up and operating.
- All of the storage paths must be available.
- You need the admin password and access to an HTTP server.
- You must be using a supported firmware version.

**NetApp Interoperability Matrix Tool**

In the IMT, you can use the Storage Solution field to select your MetroCluster solution. You use the **Component Explorer** to select the components and ONTAP version to refine your search.

You can click **Show Results** to display the list of supported configurations that match the criteria.

**About this task**

- You can use this task only on FibreBridge 7600N or 7500N bridges in configurations running ONTAP 9.4 or later.
- You must perform this task on each FibreBridge bridge in the MetroCluster configuration, so that all of the bridges are running the same firmware version.

**Note:** This procedure is nondisruptive and takes approximately 30 minutes to complete.

**Steps**

1. Invoke an AutoSupport message indicating the start of the maintenance:

   ```bash
   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. Go to the ATTO FibreBridge Description page, select your firmware version, and then follow the links and directions to download the bridge firmware.

   *NetApp Downloads: ATTO FibreBridge 7600N*

   *NetApp Downloads: ATTO FibreBridge 7500N*

3. Place the firmware file in a network location that is network accessible to the controller modules. You can enter the commands in the remaining steps from the console of either controller module.

4. Change to the advanced privilege level:

   `set -privilege advanced`

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

5. Update the bridge firmware.

   a. Update the bridge firmware by running the following commands:

      `storage bridge firmware update -name bridge-name -url URL-of-firmware-package`

      **Example**

      ```
      cluster_A> storage bridge firmware update -name bridge_A_1a -url http://192.168.132.97/firmware.spf
      ```

   b. You must run the firmware update again to make sure that both images are running the same firmware.

6. Return to the admin privilege level:

   `set -privilege admin`

7. Verify that the firmware upgrade is complete:

   `job show -name Storage bridge firmware update`

   **Example**

   The following example shows that the job is still running:

   ```
   cluster_A> job show -name storage bridge firmware update
   Owning
   Job ID Name          Vserver     Node     State
   ------ ------------- ----------- -------
   2246 job-name       cluster_A   node_A_1a Running
   Description: Storage bridge firmware update job
   ```

   After approximately 10 minutes, the new firmware is fully installed and the job state will be **Success**:

   ```
   cluster_A> job show -name Storage bridge firmware update
   Owning
   Job ID Name          Vserver     Node     State
   ------ ------------- ----------- -------
   ```
8. Complete the steps according to whether in-band management is enabled and which version of ONTAP your system is running:

- If you are running ONTAP 9.4, in-band management is not supported and the command must be issued from the bridge console:
  
a. Run the `flashimages` command on the console of the bridge and confirm that the correct firmware versions are displayed.

  **Note:** The example shows that primary flash image shows the new firmware image, while the secondary flash image shows the old image.

  ```
  flashimages
<table>
<thead>
<tr>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>2.95 012N</td>
</tr>
<tr>
<td>Secondary</td>
<td>2.90 002N</td>
</tr>
<tr>
<td>Ready</td>
<td></td>
</tr>
</tbody>
</table>
  ```

  b. Reboot the bridge by running the `firmwarerestart` command from the bridge.

- If you are running ONTAP 9.5 or later, in-band management is supported and the command can be issued from the cluster prompt:
  
a. Run the `storage bridge run-cli -name bridge-name -command FlashImages` command.

  **Note:** The example shows that primary flash image shows the new firmware image, while the secondary flash image shows the old image.

  ```
  cluster_A> storage bridge run-cli -name ATTO_7500N_IB_1 -command FlashImages
  [Job 2257]
<table>
<thead>
<tr>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>2.95 012N</td>
</tr>
<tr>
<td>Secondary</td>
<td>2.90 002N</td>
</tr>
<tr>
<td>Ready</td>
<td></td>
</tr>
</tbody>
</table>
  ```

  b. If necessary, restart the bridge: `storage bridge run-cli -name ATTO_7500N_IB_1 -command FirmwareRestart`

    **Note:** Starting with ATTO firmware version 2.95 the bridge will restart automatically and this step is not required.

9. Verify that the bridge restarted correctly:

  ```sysconfig```

  The system should be cabled for multipath high availability (both controllers have access through the bridges to the disk shelves in each stack).
10. Verify that the FibreBridge firmware was updated:
storage bridge show -fields fw-version,symbolic-name

Example

```
cluster_A> storage bridge show -fields fw-version,symbolic-name

name              fw-version        symbolic-name
----------------- ----------------- -------------
ATTO_10.0.0.1     1.63 071C 51.01   bridge_A_1a
ATTO_10.0.0.2     1.63 071C 51.01   bridge_A_1b
ATTO_10.0.1.1     1.63 071C 51.01   bridge_A_2a
ATTO_10.0.1.2     1.63 071C 51.01   bridge_A_2b
4 entries were displayed.
```

11. Verify that both partitions are updated from the bridge's prompt:
flashimages

Example

The output should show the same version for both partitions.

```
Ready.
flashimages 4
;Type         Version
;====================================================================
Primary       2.80 003T
Secondary     2.80 003T
Ready.
```

12. Repeat the previous step on the next bridge, until all of the bridges in the MetroCluster configuration have been updated.

**Updating firmware on FibreBridge 7500N on configurations running ONTAP 9.3.x and earlier or 6500N bridges**

You might need to update the firmware on your FibreBridge bridges to ensure that you have the latest features or to resolve possible issues. This procedure should be used for FibreBridge 7500N on configurations running ONTAP 9.3.x or for FibreBridge 6500N bridges on all supported versions of ONTAP.

**Before you begin**

- The MetroCluster configuration must be operating normally.
- All of the FibreBridge bridges in the MetroCluster configuration must be up and operating.
- All of the storage paths must be available.
- You need the admin password and access to an FTP or SCP server.
- You must be using a supported firmware version.

**NetApp Interoperability Matrix Tool**

In the IMT, you can use the Storage Solution field to select your MetroCluster solution. You use the Component Explorer to select the components and ONTAP version to refine your search. You can click Show Results to display the list of supported configurations that match the criteria.
About this task

You can use this task with either FibreBridge 7500N or 6500N bridges. Starting with ONTAP 9.3, you can use the ONTAP storage bridge firmware update command to update bridge firmware on FibreBridge 7500N bridges.

Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later on page 14

You must perform this task on each FibreBridge bridge in the MetroCluster configuration, so that all of the bridges are running the same firmware version.

Note: This procedure is nondisruptive and takes approximately 30 minutes to complete.

Steps

1. Invoke an AutoSupport message indicating the start of the maintenance:

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

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

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

2. Go to the ATTO FibreBridge Description page.

   NetApp Downloads: ATTO FibreBridge 7500N
   NetApp Downloads: ATTO FibreBridge 6500N

3. Using the link on the ATTO FibreBridge Description page, access the ATTO web site.

   If you are using... Then download...
   FibreBridge 7500N
     • ATTO FibreBridge 7500N Installation and Operation Manual
     • ATTO QuickNAV utility (to the computer that you are using for setup)
   FibreBridge 6500N
     • ATTO FibreBridge 6500N Installation and Operation Manual
     • ATTO QuickNAV utility (to the computer that you are using for setup)

4. Return to the ATTO FibreBridge Description page, and then click Continue at the bottom of the page to access the ATTO FibreBridge Firmware Download page.

5. Download the bridge firmware file using Steps 1 through 3 of the procedure on the ATTO FibreBridge Firmware Download page.

6. Make a copy of the ATTO FibreBridge Firmware Download page and release notes for reference when you are instructed to update the firmware on each bridge.

7. Update the bridge:

   a. Install the firmware on the FibreBridge bridge.

      • If you are using ATTO FibreBridge 7500N bridges, you should refer to the instructions provided in the “Update Firmware” section of the ATTO FibreBridge 7500N Installation and Operation Manual.
• If you are using ATTO FibreBridge 6500N bridges, you should refer to the instructions provided in the “Update Firmware” section of the *ATTO FibreBridge 6500N Installation and Operation Manual*.

**Attention:** You should be sure to power-cycle the individual bridge now. If you wait and power-cycle both bridges in a stack simultaneously, the controller might lose access to the drives, resulting in a plex failure or multidisk panic.

The bridge should restart.

b. From the console of either controller, verify that the bridge restarted correctly:

```
sysconfig
```

The system should be cabled for multipath high availability (both controllers have access through the bridges to the disk shelves in each stack).

**Example**

```
cluster_A::> node run -node cluster_A-01 -command sysconfig
System ID: 1234567890 (cluster_A-01); partner ID: 0123456789 (cluster_A-02)
System Serial Number: 200012345678 (cluster_A-01)
System Rev: A4
System Storage Configuration: Quad-Path HA
```

c. From the console of either controller, verify that the FibreBridge firmware was updated:

```
storage bridge show -fields fw-version,symbolic-name
```

**Example**

```
cluster_A::> storage bridge show -fields fw-version,symbolic-name
name          fw-version        symbolic-name
-------------- ----------------- ---------------
ATTO_10.0.0.1  1.63 071C 51.01   bridge_A_1a
ATTO_10.0.0.2  1.63 071C 51.01   bridge_A_1b
ATTO_10.0.1.1  1.63 071C 51.01   bridge_B_1a
ATTO_10.0.1.2  1.63 071C 51.01   bridge_B_1b
4 entries were displayed.
```

d. Repeat the previous substeps on the same bridge to update the second partition.

e. Verify that both partitions are updated:

```
flashimages
```

**Example**

```
Ready.
flashimages
4
;Type         Version
;=================================================================
Primary       2.80 003T
Secondary     2.80 003T
Ready.
```

8. Repeat the previous step on the next bridge, until all of the bridges in the MetroCluster configuration have been updated.
Replacing a single FC-to-SAS bridge

You can nondisruptively replace a bridge with a same model bridge or with a new model bridge.

Before you begin

You need the admin password and access to an FTP or SCP server.

About this task

This procedure is nondisruptive and takes approximately 60 minutes to complete.

This procedure uses the bridge CLI to configure and manage a bridge, and to update the bridge firmware and the ATTO QuickNA V utility to configure the bridge Ethernet management 1 port. You can use other interfaces if they meet the requirements.

Requirements for using other interfaces to configure and manage FibreBridge bridges on page 58

Choices

• Verifying storage connectivity on page 20
• Hot-swapping a bridge with a replacement bridge of the same model on page 21
• Hot-swapping a FibreBridge 7500N with a 7600N bridge on page 27
• Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge on page 33

Related tasks

Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges on page 39

Verifying storage connectivity

Before replacing bridges, you should verify bridge and storage connectivity. Familiarizing yourself with the command output enables you to subsequently confirm connectivity after making configuration changes.

About this task

You can issue these commands from the admin prompt of any of the controller modules in the MetroCluster configuration at the site undergoing maintenance.

Step

1. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:

   run local sysconfig -v

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

   Example

   node_A.1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
   System ID: 4568741258 (node_A.1); partner ID: 4068741260 (node_B.1)
   System Serial Number: 940001025471 (node_A.1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA<<< Configuration should be multi-path HA
   .
   .
   .
Hot-swapping a bridge with a replacement bridge of the same model

You can hot-swap a failed bridge with another bridge of the same model.

About this task

If you will be using in-band management of the bridge rather than IP management, the steps for configuring the Ethernet port and IP settings can be skipped, as noted in the relevant steps.

Steps

1. If the bridge is in a fabric-attached MetroCluster configuration, disable all of the switch ports that connect to the bridge FC port or ports.

2. From the ONTAP cluster prompt, remove the bridge undergoing maintenance from health monitoring:
   a. Remove the bridge:
      ```
      storage bridge remove -name bridge-name
      ```
   b. View the list of monitored bridges and confirm that the removed bridge is not present:
      ```
      storage bridge show
      ```

3. Properly ground yourself.

4. Power down the ATTO bridge.

<table>
<thead>
<tr>
<th>If you are using a...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreBridge 7600N or 7500N bridge</td>
<td>Remove the power cables connected to the bridge.</td>
</tr>
<tr>
<td>FibreBridge 6500N bridge</td>
<td>Turn off the power switch of the bridge.</td>
</tr>
</tbody>
</table>

5. Disconnect the cables that are connected to the old bridge.

You should make note of the port to which each cable was connected.
6. Remove the old bridge from the rack.

7. Install the new bridge into the rack.

8. Reconnect the power cord and, if configuring for IP access to the bridge, a shielded Ethernet cable.

   **Attention:** You must not reconnect the SAS or FC cables at this time.

9. Connect the bridge to a power source, and then turn it on.

   The bridge Ready LED might take up to 30 seconds to illuminate, indicating that the bridge has completed its power-on self test sequence.

10. If configuring for in-band management, connect a cable from FibreBridge RS-232 serial port to the serial (COM) port on a personal computer.

    The serial connection will be used for initial configuration, and then in-band management via ONTAP and the FC ports can be used to monitor and manage the bridge.

11. If configuring for IP management, configure the Ethernet management 1 port for each bridge by following the procedure in section 2.0 of the *ATTO FibreBridge Installation and Operation Manual* for your bridge model.

    In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.

    When running QuickNAV to configure an Ethernet management port, only the Ethernet management port that is connected by the Ethernet cable is configured. For example, if you also wanted to configure the Ethernet management 2 port, you would need to connect the Ethernet cable to port 2 and run QuickNAV.

12. Configure the bridge.

   Be sure to make note of the user name and password that you designate.

   The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

   **Note:** Do not configure time synchronization on ATTO FibreBridge 7600N or 7500N. The time synchronization for ATTO FibreBridge 7600N or 7500N is set to the cluster time after the bridge is discovered by ONTAP. It is also synchronized periodically once a day. The time zone used is GMT and is not changeable.

   a. If configuring for IP management, configure the IP settings of the bridge.

      To set the IP address without the QuickNAV utility, you need to have a serial connection to the FibreBridge.

      **Example**

      If using the CLI, you must run the following commands:

      ```
      set ipaddress m1 ip-address
      set ipsubnetmask m1 subnet-mask
      set ipgateway m1 x.x.x.x
      set ipdhcp m1 disabled
      set ethernetspeed m1 1000
      ```

   b. Configure the bridge name.

      The bridges should each have a unique name within the MetroCluster configuration.

      Example bridge names for one stack group on each site:

      ```
      22
      | MetroCluster Service and Expansion Guide
      ```
- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

**Example**

If using the CLI, you must run the following command:

```
set bridgename bridgename
```

c. If running ONTAP 9.4 or earlier, enable SNMP on the bridge:

```
set SNMP enabled
```

If running ONTAP 9.5 or later, ONTAP will use in-band monitoring via the FC connection to the bridge, so you should leave SNMP disabled.

13. Configure the bridge FC ports.

a. Configure the data rate/speed of the bridge FC ports.

   The supported FC data rate depends on your model bridge.
   
   - The FibreBridge 7600 bridge supports up to 32, 16, or 8 Gbps.
   - The FibreBridge 7500 bridge supports up to 16, 8, or 4 Gbps.
   - The FibreBridge 6500 bridge supports up to 8, 4, or 2 Gbps.

   **Note:** The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

   **Example**

   If using the CLI, you must run the following command:

   ```
   set FCDataRate port-number port-speed
   ```

b. If you are configuring a FibreBridge 7500N or 6500N bridge, configure the connection mode that the port uses to ptp.

   **Note:** The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

   **Example**

   If using the CLI, you must run the following command:

   ```
   set FCConnMode port-number ptp
   ```

c. If you are configuring a FibreBridge 7600N or 7500N bridge, you must configure or disable the FC2 port.

   - If you are using the second port, you must repeat the previous substeps for the FC2 port.
   - If you are not using the second port, then you must disable the port:

     ```
     FCPortDisable port-number
     ```

d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports:

   ```
   SASPortDisable sas-port
   ```
Note: SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used. If only SAS port A is used, then SAS ports B, C, and D must be disabled.

14. Save the bridge's configuration and secure the bridge.
   a. Save the bridge's configuration.

   Example
   You must run the following commands:
   - `SaveConfiguration`
   - `FirmwareRestart`
   You are prompted to restart the bridge.

   b. If running ONTAP 9.5 or later, secure access to the bridge.
   Starting with ONTAP 9.5, you can secure access to the bridge to allow access only using in-band management through the FC ports.

   Example
   You must run the following command:
   - `SecureBridge`

15. Update the FibreBridge firmware on each bridge.

16. Reconnect the SAS and FC cables to the same ports on the new bridge.
   If the new bridge is a FibreBridge 7600N or 7500N, you must replace the cables connecting the bridge to the top or bottom of the shelf stack. The FibreBridge 6500N bridge used SAS cables; the FibreBridge 7600N and 7500N bridges require mini-SAS cables for these connections.

   Note: Wait at least 10 seconds before connecting the port. The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place and the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector). For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

17. Verify that each bridge can see all of the disk drives and disk shelves to which the bridge is connected.

<table>
<thead>
<tr>
<th>If you are using the...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTO ExpressNAV GUI</td>
<td>a. In a supported web browser, enter the IP address of the bridge in the browser box. You are brought to the ATTO FibreBridge homepage, which has a link.</td>
</tr>
<tr>
<td></td>
<td>b. Click the link, and then enter your user name and the password that you designated when you configured the bridge. The ATTO FibreBridge status page appears with a menu to the left.</td>
</tr>
<tr>
<td></td>
<td>c. Click Advanced in the menu.</td>
</tr>
<tr>
<td></td>
<td>d. View the connected devices: <code>sastargets</code></td>
</tr>
<tr>
<td></td>
<td>e. Click Submit.</td>
</tr>
</tbody>
</table>
### If you are using the...

<table>
<thead>
<tr>
<th>Serial port connection</th>
<th>View the connected devices:</th>
</tr>
</thead>
</table>

The output shows the devices (disks and disk shelves) to which the bridge is connected. The output lines are sequentially numbered so that you can quickly count the devices.

**Note:** If the text `response truncated` appears at the beginning of the output, you can use Telnet to connect to the bridge, and then view all of the output by using the `sastargets` command.

### Example

The following output shows that 10 disks are connected:

<table>
<thead>
<tr>
<th>Tgt</th>
<th>VendorID</th>
<th>ProductID</th>
<th>Type</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CLE300009940UHJV</td>
</tr>
<tr>
<td>1</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1ELF600009940V1BV</td>
</tr>
<tr>
<td>2</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G3EW00009940U2M0</td>
</tr>
<tr>
<td>3</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1EWM00009940U1X5</td>
</tr>
<tr>
<td>4</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLE00009940G8YU</td>
</tr>
<tr>
<td>5</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLF00009940TIZK</td>
</tr>
<tr>
<td>6</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CEB400009939MGXL</td>
</tr>
<tr>
<td>7</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G7A900009939FNTT</td>
</tr>
<tr>
<td>8</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FY0T00009940GBPA</td>
</tr>
<tr>
<td>9</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FXW600009940VERQ</td>
</tr>
</tbody>
</table>

18. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

### If the output is...

<table>
<thead>
<tr>
<th>Correct</th>
<th>Repeat Step 17 on page 24 for each remaining bridge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not correct</td>
<td>a. Check for loose SAS cables or correct the SAS cabling by repeating Step 16 on page 24.</td>
</tr>
<tr>
<td></td>
<td>b. Repeat Step 17 on page 24.</td>
</tr>
</tbody>
</table>

19. If the bridge is in a fabric-attached MetroCluster configuration, reenable the FC switch port that you disabled at the beginning of this procedure. This should be the port that connects to the bridge.

20. From the system console of both controller modules, verify that all of the controller modules have access through the new bridge to the disk shelves (that is, that the system is cabled for Multipath HA):

   ```
   run local sysconfig
   ```

   **Note:** It might take up to a minute for the system to complete discovery.

   If the output does not indicate Multipath HA, you must correct the SAS and FC cabling because not all of the disk drives are accessible through the new bridge.

### Example

The following output states that the system is cabled for Multipath HA:
Attention: When the system is not cabled as Multipath HA, restarting a bridge might cause loss of access to the disk drives and result in a multi-disk panic.

21. If running ONTAP 9.4 or earlier, verify that the bridge is configured for SNMP.

Example
If you are using the bridge CLI, run the following command:

```
get snmp
```

22. From the ONTAP cluster prompt, add the bridge to health monitoring:

a. Add the bridge, using the command for your version of ONTAP:

<table>
<thead>
<tr>
<th>ONTAP version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 and later</td>
<td><code>storage bridge add -address 0.0.0.0 -managed-by in-band -name bridge-name</code></td>
</tr>
<tr>
<td>9.4 and earlier</td>
<td><code>storage bridge add -address bridge-ip-address -name bridge-name</code></td>
</tr>
</tbody>
</table>

b. Verify that the bridge has been added and is properly configured:

```
storage bridge show
```

It might take as long as 15 minutes to reflect all data because of the polling interval. The ONTAP health monitor can contact and monitor the bridge if the value in the Status column is ok, and other information, such as the worldwide name (WWN), is displayed.

Example
The following example shows that the FC-to-SAS bridges are configured:

```
controller_A_1::> storage bridge show

Bridge Model          Symbolic Name  Is Monitored Monitor Status  Vendor
Model                  Name           WWN              Bridge WWN            Status            Vendor
--------------------  -------------  ------------  ------------  --------  ----------
ATTO_10.10.20.10      atto01        true          ok              Atto   FibreBridge
7500N                  20000010867038c0
ATTO_10.10.20.11      atto02        true          ok              Atto   FibreBridge
7500N                  20000010867033c0
ATTO_10.10.20.12      atto03        true          ok              Atto   FibreBridge
7500N                  20000010867030c0
ATTO_10.10.20.13      atto04        true          ok              Atto   FibreBridge
7500N                  2000001086703b80
4 entries were displayed
controller_A_1::>
```

23. 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:
   
   ```bash
   system health alert show
   ```

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

d. Perform a MetroCluster check:
   
   ```bash
   metrocluster check run
   ```

e. Display the results of the MetroCluster check:
   
   ```bash
   metrocluster check show
   ```

f. Run Config Advisor.
   
   ```
   NetApp Downloads: Config Advisor
   ```

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

**Related concepts**

*In-band management of the FC-to-SAS bridges* on page 59

**Hot-swapping a FibreBridge 7500N with a 7600N bridge**

You can hot-swap a FibreBridge 7500N bridge with a 7600N bridge.

**About this task**

If you will be using in-band management of the bridge rather than IP management, the steps for configuring the Ethernet port and IP settings can be skipped, as noted in the relevant steps.

**Steps**

1. If the bridge is in a fabric-attached MetroCluster configuration, disable all of the switch ports that connect to the bridge FC port or ports.

2. From the ONTAP cluster prompt, remove the bridge undergoing maintenance from health monitoring:
   
   a. Remove the bridge:
      
      ```bash
      storage bridge remove -name bridge-name
      ```
   
   b. View the list of monitored bridges and confirm that the removed bridge is not present:
      
      ```bash
      storage bridge show
      ```

3. Properly ground yourself.

4. Remove the power cables connected to the bridge to power down the bridge.

5. Disconnect the cables that are connected to the old bridge.
   
   You should make note of the port to which each cable was connected.

6. Remove the old bridge from the rack.

7. Install the new bridge into the rack.

8. Reconnect the power cord and shielded Ethernet cable.

   **Attention:** You must not reconnect the SAS or FC cables at this time.
9. Connect the bridge to a power source, and then turn it on.
     The bridge Ready LED might take up to 30 seconds to illuminate, indicating that the bridge has completed its power-on self test sequence.

10. If configuring for in-band management, connect a cable from FibreBridge RS-232 serial port to the serial (COM) port on a personal computer.
     The serial connection will be used for initial configuration, and then in-band management via ONTAP and the FC ports can be used to monitor and manage the bridge.

11. If configuring for in-band management, connect a cable from FibreBridge RS-232 serial port to the serial (COM) port on a personal computer.
     The serial connection will be used for initial configuration, and then in-band management via ONTAP and the FC ports can be used to monitor and manage the bridge.

12. If configuring for IP management, configure the Ethernet management 1 port for each bridge by following the procedure in section 2.0 of the *ATTO FibreBridge Installation and Operation Manual* for your bridge model.
     In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.
     When running QuickNAV to configure an Ethernet management port, only the Ethernet management port that is connected by the Ethernet cable is configured. For example, if you also wanted to configure the Ethernet management 2 port, you would need to connect the Ethernet cable to port 2 and run QuickNAV.

13. Configure the bridges.
     Be sure to make note of the user name and password that you designate.
     The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

     **Note:** Do not configure time synchronization on FibreBridge 7600N. The time synchronization for FibreBridge 7600N is set to the cluster time after the bridge is discovered by ONTAP. It is also synchronized periodically once a day. The time zone used is GMT and is not changeable.

     a. If configuring for IP management, configure the IP settings of the bridge.
     To set the IP address without the QuickNAV utility, you need to have a serial connection to the FibreBridge.

     **Example**
     If using the CLI, you must run the following commands:
     ```
     set ipaddress mpl ip-address
     set ipsubnetmask mpl subnet-mask
     set ipgateway mpl x.x.x.x
     set ipdhcp mpl disabled
     set ethnetspeed mpl 1000
     ```

     b. Configure the bridge name.
     The bridges should each have a unique name within the MetroCluster configuration.
     Example bridge names for one stack group on each site:
     - bridge_A_1a
     - bridge_A_1b
• bridge_B_1a
• bridge_B_1b

Example
If using the CLI, you must run the following command:

```
set bridgename" bridgename
```

c. If running ONTAP 9.4 or earlier, enable SNMP on the bridge:

```
set SNMP enabled
```

If running ONTAP 9.5 or later, ONTAP will use in-band monitoring via the FC connection to the bridge, so you should leave SNMP disabled.

14. Configure the bridge FC ports.

a. Configure the data rate/speed of the bridge FC ports.

The supported FC data rate depends on your model bridge.

- The FibreBridge 7600 bridge supports up to 32, 16, or 8 Gbps.
- The FibreBridge 7500 bridge supports up to 16, 8, or 4 Gbps.
- The FibreBridge 6500 bridge supports up to 8, 4, or 2 Gbps.

**Note:** The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the FC port of the controller module or switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

Example
If using the CLI, you must run the following command:

```
set FCDataRate port-number port-speed
```

b. You must configure or disable the FC2 port.

- If you are using the second port, you must repeat the previous substeps for the FC2 port.
- If you are not using the second port, then you must disable the unused port:

  ```
  FCPortDisable port-number
  ```

**Example**

The following example shows the disabling of FC port 2:

```
FCPortDisable 2
```

*Fibre Channel Port 2 has been disabled.*

c. Disable the unused SAS ports:

```
SASPortDisable sas-port
```

**Note:** SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used.
If only SAS port A is used, then SAS ports B, C, and D must be disabled. The following example shows disabling of SAS port B. You must similarly disable SAS ports C and D:

```plaintext
SASPortDisable b
SAS Port B has been disabled.
```

15. Save the bridge's configuration and secure the bridge.

   a. Save the bridge's configuration.

      Example
      You must run the following commands:
      ```plaintext
      SaveConfiguration
      FirmwareRestart
      ```
      You are prompted to restart the bridge.

   b. If running ONTAP 9.5 or later, secure access to the bridge.
      Starting with ONTAP 9.5, you can secure access to the bridge to allow access only using in-band management through the FC ports.

      Example
      You must run the following command:
      ```plaintext
      SecureBridge
      ```

16. Update the FibreBridge firmware on each bridge.

    Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later on page 14

17. Reconnect the SAS and FC cables to the same ports on the new bridge.

    Note: Wait at least 10 seconds before connecting the port. The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place and the disk shelf SAS port LINK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector). For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

18. Verify that each bridge can see all of the disk drives and disk shelves to which the bridge is connected:

    sastargets

    The output shows the devices (disks and disk shelves) to which the bridge is connected. The output lines are sequentially numbered so that you can quickly count the devices.

    Example
    The following output shows that 10 disks are connected:

    ```plaintext
    Tgt VendorID ProductID        Type        SerialNumber
    0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
    1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
    2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
    3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
    ```
19. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

<table>
<thead>
<tr>
<th>If the output is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Repeat the previous step for each remaining bridge.</td>
</tr>
</tbody>
</table>
| Not correct         | a. Check for loose SAS cables or correct the SAS cabling by repeating Step 16 on page 24.  
|                     | b. Repeat the previous step. |

20. If the bridge is in a fabric-attached MetroCluster configuration, reenable the FC switch port that you disabled at the beginning of this procedure.

This should be the port that connects to the bridge.

21. From the system console of both controller modules, verify that all of the controller modules have access through the new bridge to the disk shelves (that is, that the system is cabled for Multipath HA):

```
run local sysconfig
```

**Note:** It might take up to a minute for the system to complete discovery.

If the output does not indicate Multipath HA, you must correct the SAS and FC cabling because not all of the disk drives are accessible through the new bridge.

**Example**

The following output states that the system is cabled for Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016  
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)  
System Serial Number: 700000123123 (node_A_1); partner Serial Number: 700000456456 (node_A_2)  
System Rev: B0  
System Storage Configuration: Multi-Path HA  
System ACP Connectivity: NA
```

**Attention:** When the system is not cabled as Multipath HA, restarting a bridge might cause loss of access to the disk drives and result in a multi-disk panic.

22. If running ONTAP 9.4 or earlier, verify that the bridge is configured for SNMP.

**Example**

If you are using the bridge CLI, run the following command:

```
get snmp
```

23. From the ONTAP cluster prompt, add the bridge to health monitoring:

a. Add the bridge, using the command for your version of ONTAP:
### Table

<table>
<thead>
<tr>
<th>ONTAP version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 and later</td>
<td><code>storage bridge add -address 0.0.0.0 -managed-by in-band -name bridge-name</code></td>
</tr>
<tr>
<td>9.4 and earlier</td>
<td><code>storage bridge add -address bridge-ip-address -name bridge-name</code></td>
</tr>
</tbody>
</table>

b. Verify that the bridge has been added and is properly configured:

```
storage bridge show
```

It might take as long as 15 minutes to reflect all data because of the polling interval. The ONTAP health monitor can contact and monitor the bridge if the value in the Status column is `ok`, and other information, such as the worldwide name (WWN), is displayed.

### Example

The following example shows that the FC-to-SAS bridges are configured:

```
controller_A_1::> storage bridge show

<table>
<thead>
<tr>
<th>Bridge Model</th>
<th>Symbolic Name</th>
<th>Is Monitored</th>
<th>Monitor Status</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTO_10.10.20.10</td>
<td>atto01</td>
<td>true</td>
<td>ok</td>
<td>Atto FibreBridge</td>
</tr>
<tr>
<td>7500N</td>
<td>20000010867038c0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTO_10.10.20.11</td>
<td>atto02</td>
<td>true</td>
<td>ok</td>
<td>Atto FibreBridge</td>
</tr>
<tr>
<td>7500N</td>
<td>20000010867033c0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTO_10.10.20.12</td>
<td>atto03</td>
<td>true</td>
<td>ok</td>
<td>Atto FibreBridge</td>
</tr>
<tr>
<td>7500N</td>
<td>20000010867030c0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTO_10.10.20.13</td>
<td>atto04</td>
<td>true</td>
<td>ok</td>
<td>Atto FibreBridge</td>
</tr>
<tr>
<td>7500N</td>
<td>2000001086703b80</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 entries were displayed
```

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

   a. Check whether the system is multipathed:
      ```
      node run -node (node name) sysconfig -a
      ```

   b. Check for any health alerts on both clusters:
      ```
      system health alert show
      ```

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

   d. Perform a MetroCluster check:
      ```
      metrocluster check run
      ```

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

   f. Run Config Advisor.
      ```
      NetApp Downloads: Config Advisor
      ```

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

*In-band management of the FC-to-SAS bridges* on page 59

**Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge**

You can hot-swap a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge to replace a failed bridge or upgrade your bridge in a fabric-attached or a bridge-attached MetroCluster configuration.

**About this task**

- This procedure is for hot-swapping a single FibreBridge 6500N bridge with single FibreBridge 7600N or 7500N bridge.

- When you hot-swap a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge, you must use only one FC port and one SAS port on the FibreBridge 7600N or 7500N bridge.

- If you will be using in-band management of the bridge rather than IP management, the steps for configuring the Ethernet port and IP settings can be skipped, as noted in the relevant steps.

**Attention:** If you are hot-swapping both FibreBridge 6500N bridges in a pair, you must use the *Consolidate Multiple Storage Stacks* on page 39 procedure for zoning instructions. By replacing both FibreBridge 6500N bridges on the bridge, you can take advantage of the additional ports on the FibreBridge 7600N or 7500N bridge.

**Steps**

1. Do one of the following:
   - If the failed bridge is in a fabric-attached MetroCluster configuration, disable the switch port that connects to the bridge FC port.
   - If the failed bridge is in a stretch Metrocluster configuration, use either one of the available FC ports.

2. From the ONTAP cluster prompt, remove the bridge undergoing maintenance from health monitoring:
   a. Remove the bridge:
      ```
      storage bridge remove -name bridge-name
      ```
   b. View the list of monitored bridges and confirm that the removed bridge is not present:
      ```
      storage bridge show
      ```

3. Properly ground yourself.

4. Turn off the power switch of the bridge.

5. Disconnect the cables connected from the shelf to the FibreBridge 6500N bridge ports and power cables.
   You should make note of the ports that each cable was connected to.

6. Remove the FibreBridge 6500N bridge that you need to replace from the rack.

7. Install the new FibreBridge 7600N or 7500N bridge into the rack.

8. Reconnect the power cord and, if necessary, the shielded Ethernet cable.

**Attention:** Do not reconnect the SAS or FC cables at this time.
9. If configuring for in-band management, connect a cable from FibreBridge RS-232 serial port to the serial (COM) port on a personal computer.

The serial connection will be used for initial configuration, and then in-band management via ONTAP and the FC ports can be used to monitor and manage the bridge.

10. If configuring for IP management, connect the Ethernet management 1 port on each bridge to your network by using an Ethernet cable.

In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.

The Ethernet management 1 port enables you to quickly download the bridge firmware (using ATTO ExpressNAV or FTP management interfaces) and to retrieve core files and extract logs.

11. If configuring for IP management, configure the Ethernet management 1 port for each bridge by following the procedure in section 2.0 of the ATTO FibreBridge Installation and Operation Manual for your bridge model.

In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.

When running QuickNAV to configure an Ethernet management port, only the Ethernet management port that is connected by the Ethernet cable is configured. For example, if you also wanted to configure the Ethernet management 2 port, you would need to connect the Ethernet cable to port 2 and run QuickNAV.

12. Configure the bridge.

Be sure to make note of the user name and password that you designate.

The ATTO FibreBridge Installation and Operation Manual for your bridge model has the most current information on available commands and how to use them.

Note: Do not configure time synchronization on ATTO FibreBridge 7600N or 7500N. The time synchronization for ATTO FibreBridge 7600N or 7500N is set to the cluster time after the bridge is discovered by ONTAP. It is also synchronized periodically once a day. The time zone used is GMT and is not changeable.

a. If configuring for IP management, configure the IP settings of the bridge.

To set the IP address without the QuickNAV utility, you need to have a serial connection to the FibreBridge.

Example

If using the CLI, you must run the following commands:

```
set ipaddress mpl ip-address
set ipsubnetmask mpl subnet-mask
set ipgateway mpl x.x.x.x
set ipdhcp mpl disabled
set ethernetspeed mpl 1000
```

b. Configure the bridge name.

The bridges should each have a unique name within the MetroCluster configuration.

Example bridge names for one stack group on each site:

- bridge_A_1a
- bridge_A_1b
• bridge_B_1a
• bridge_B_1b

**Example**
If using the CLI, you must run the following command:

`set bridgename bridgename`

c. If running ONTAP 9.4 or earlier, enable SNMP on the bridge:

`set SNMP enabled`

If running ONTAP 9.5 or later, ONTAP will use in-band monitoring via the FC connection to the bridge, so you should leave SNMP disabled.

13. Configure the bridge FC ports.

a. Configure the data rate/speed of the bridge FC ports.

The supported FC data rate depends on your model bridge.

• The FibreBridge 7600 bridge supports up to 32, 16, or 8 Gbps.
• The FibreBridge 7500 bridge supports up to 16, 8, or 4 Gbps.
• The FibreBridge 6500 bridge supports up to 8, 4, or 2 Gbps.

**Note:** The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

**Example**
If using the CLI, you must run the following command:

`set FCDataRate port-number port-speed`

b. If you are configuring a FibreBridge 7500N or 6500N bridge, configure the connection mode that the port uses to ptp.

**Note:** The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

**Example**
If using the CLI, you must run the following command:

`set FCConnMode port-number ptp`

c. If you are configuring a FibreBridge 7600N or 7500N bridge, you must configure or disable the FC2 port.

• If you are using the second port, you must repeat the previous substeps for the FC2 port.
• If you are not using the second port, then you must disable the port:

`FCPortDisable port-number`

d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports:

`SASPortDisable sas-port`
Note: SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used. If only SAS port A is used, then SAS ports B, C, and D must be disabled.

14. Save the bridge’s configuration and secure the bridge.
   a. Save the bridge’s configuration.

   Example
   You must run the following commands:
   `SaveConfiguration`
   `FirmwareRestart`
   You are prompted to restart the bridge.

   b. If running ONTAP 9.5 or later, secure access to the bridge.
   Starting with ONTAP 9.5, you can secure access to the bridge to allow access only using in-band management through the FC ports.

   Example
   You must run the following command:
   `SecureBridge`

15. Turn on Health Monitoring for the FibreBridge 7600N or 7500N bridge.

16. Update the FibreBridge firmware on each bridge.

17. Reconnect the SAS and FC cables to the SAS A and Fibre Channel 1 ports on the new bridge.
   The SAS port must be cabled to the same shelf port that the FibreBridge 6500N bridge had been connected to.
   The FC port must be cabled to the same switch or controller port that the FibreBridge 6500N bridge had been connected to.

   Note: Do not force a connector into a port. The mini-SAS cables are keyed; when oriented correctly into a SAS port, the SAS cable clicks into place and the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector). For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

18. Verify that the bridge can see all of the disk drives and disk shelves it is connected to.
If you are using the ATTO ExpressNAV GUI

a. In a supported web browser, enter the IP address of the bridge in the browser box. You are brought to the ATTO FibreBridge homepage, which has a link.

b. Click the link, and then enter your user name and the password that you designated when you configured the bridge. The ATTO FibreBridge status page appears with a menu to the left.

c. Click Advanced in the menu.

d. Enter the following command and then click Submit to see the list of disks visible to the bridge:

```
sastargets
```

Serial port connection

Display the list of disks visible to the bridge:

```
sastargets
```

Example

The output shows the devices (disks and disk shelves) that the bridge is connected to. Output lines are sequentially numbered so that you can quickly count the devices. For example, the following output shows that 10 disks are connected:

<table>
<thead>
<tr>
<th>Tgt</th>
<th>VendorID</th>
<th>ProductID</th>
<th>Type</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CLE300009940UHVJ</td>
</tr>
<tr>
<td>1</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1ELF60009940V1BV</td>
</tr>
<tr>
<td>2</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G3EW00009940U2M0</td>
</tr>
<tr>
<td>3</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1EWMP00009940U1X5</td>
</tr>
<tr>
<td>4</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLE00009940G8YU</td>
</tr>
<tr>
<td>5</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLF00009940TZKZ</td>
</tr>
<tr>
<td>6</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G7A90000993XFNTT</td>
</tr>
<tr>
<td>7</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FY0T00009940G8PA</td>
</tr>
<tr>
<td>8</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FXW600009940VERQ</td>
</tr>
</tbody>
</table>

Note: If the text response truncated appears at the beginning of the output, you can use Telnet to access the bridge and enter the same command to see all of the output.

19. Verify that the command output shows that the bridge is connected to all of the necessary disks and disk shelves in the stack.

If the output is...

<table>
<thead>
<tr>
<th>Correct</th>
<th>Then... Repeat Step 18 on page 36 for each remaining bridge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not correct</td>
<td>a. Check for loose SAS cables or correct the SAS cabling by repeating Step 17 on page 36.</td>
</tr>
<tr>
<td></td>
<td>b. Repeat Step 18 on page 36.</td>
</tr>
</tbody>
</table>

20. Reenable the FC switch port that connects to the bridge.

21. Verify that all controllers have access through the new bridge to the disk shelves (that the system is cabled for Multipath HA), at the system console of both controllers:

```
run local sysconfig
```

Note: It might take up to a minute for the system to complete discovery.
For example, the following output shows that the system is cabled for Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:23:24 PST 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

If the command output indicates that the configuration is mixed-path or single-path HA, you must correct the SAS and FC cabling because not all disk drives are accessible through the new bridge.

**Attention:** When the system is not cabled as Multipath HA, restarting a bridge might cause loss of access to the disk drives and result in a multi-disk panic.

22. From the ONTAP cluster prompt, add the bridge to health monitoring:

a. Add the bridge, using the command for your version of ONTAP:

```
<table>
<thead>
<tr>
<th>ONTAP version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 and later</td>
<td>storage bridge add -address 0.0.0.0 -managed-by in-band -name bridge-name</td>
</tr>
<tr>
<td>9.4 and earlier</td>
<td>storage bridge add -address bridge-ip-address -name bridge-name</td>
</tr>
</tbody>
</table>
```

b. Verify that the bridge has been added and is properly configured:

```
storage bridge show
```

It might take as long as 15 minutes to reflect all data because of the polling interval. The ONTAP health monitor can contact and monitor the bridge if the value in the Status column is ok, and other information, such as the worldwide name (WWN), is displayed.

**Example**

The following example shows that the FC-to-SAS bridges are configured:

```
controller_A_1::> storage bridge show
```

```
<table>
<thead>
<tr>
<th>Bridge Model</th>
<th>Symbolic Name Is Monitored</th>
<th>Monitor Status</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTO_10.10.20.10 7500N</td>
<td>atto01 20000010867038c0</td>
<td>true</td>
<td>ok</td>
</tr>
<tr>
<td>ATTO_10.10.20.11 7500N</td>
<td>atto02 20000010867033c0</td>
<td>true</td>
<td>ok</td>
</tr>
<tr>
<td>ATTO_10.10.20.12 7500N</td>
<td>atto03 20000010867030c0</td>
<td>true</td>
<td>ok</td>
</tr>
<tr>
<td>ATTO_10.10.20.13 7500N</td>
<td>atto04 2000001086703b80</td>
<td>true</td>
<td>ok</td>
</tr>
</tbody>
</table>
```

4 entries were displayed

```
controller_A_1::>
```

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

a. Check whether the system is multipathed:

```
node run -node (node name) sysconfig -a
```

b. Check for any health alerts on both clusters:

```
system health alert show
```
c. Confirm the MetroCluster configuration and that the operational mode is normal:
   
   `metrocluster show`

d. Perform a MetroCluster check:
   
   `metrocluster check run`

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

f. Run Config Advisor.

   `NetApp Downloads: Config Advisor`

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

24. Return the failed part to NetApp as described in the RMA instructions shipped with the kit.

   Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

**Related concepts**

- *In-band management of the FC-to-SAS bridges* on page 59

---

### Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges

To take advantage of the additional FC2 port on the FibreBridge 7600N or 7500N bridges and reduce rack utilization, you can nondisruptively replace 6500N bridges and consolidate up to four storage stacks behind a single pair of FibreBridge 7600N or 7500N bridges.

**Before you begin**

You need the admin password and access to an FTP or SCP server.

**About this task**

You should use this procedure if:

- You are replacing a pair of FibreBridge 6500N bridges with FibreBridge 7600N or 7500N bridges.
  - After the replacement, both bridges in the pair must be the same model.
- You previously replaced a single FibreBridge 6500N bridge with a 7600N or 7500N bridge and are now replacing the second bridge in the pair.
- You have a pair of FibreBridge 7600N or 7500N bridges with available SAS ports and you are consolidating SAS storage stacks that are currently connected using FibreBridge 6500N bridges.

This procedure is nondisruptive and takes approximately two hours to complete.

**Steps**

1. [Verifying storage connectivity](#) on page 40
2. [Hot-swapping FibreBridge 6500N bridges to create a pair of FibreBridge 7600N or 7500N bridges](#) on page 41
3. Cabling the bridge SAS ports when consolidating storage behind FibreBridge 7600N or 7500N bridges on page 46
4. Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration on page 50
5. Cabling the second bridge FC port when adding FibreBridge 7600N or 7500N bridges to a configuration on page 54
6. Disabling unused SAS ports on the FC-to-SAS bridges on page 57

Related tasks

Replacing a single FC-to-SAS bridge on page 20

Verifying storage connectivity

Before replacing bridges, you should verify bridge and storage connectivity. Familiarizing yourself with the command output enables you to subsequently confirm connectivity after making configuration changes.

About this task

You can issue these commands from the admin prompt of any of the controller modules in the MetroCluster configuration at the site undergoing maintenance.

Step

1. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:

   ```bash
   run local sysconfig -v
   ```

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

   ![Example](image)

   ```bash
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
   System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
   System Serial Number: 940001025471 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA
   
   slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)
   Firmware rev:      7.5.0
   Flash rev:         0.0.0
   Host Port Id:      0x60130
   FC Node Name:      5:00a:098201:bae312
   FC Port Name:      5:00a:098201:bae312
   SFP Vendor:        UTILITIES CORP.
   SFP Part Number:   FTLF8529P3BCVAN1
   SFP Serial Number: URQ0Q9R
   SFP Capabilities:  4, 8 or 16 Gbit
   Link Data Rate:    16 Gbit
   Switch Port:       brcd6505-fcs40:1
   
   <List of disks visible to port>
   ID     Vendor   Model            FW    Size
   brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04 847.5GB
   brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02 847.5GB
   
   <List of FC-to-SAS bridges visible to port>
   FC-to-SAS Bridge:  
   brcd6505-fcs40:12.126L0 : ATTO FibreBridge6500N 1.61 FB6500N102980
   brcd6505-fcs42:13.126L0 : ATTO FibreBridge6500N 1.61 FB6500N102980
   brcd6505-fcs42:6.126L0 : ATTO FibreBridge6500N 1.61 FB6500N101167
   brcd6505-fcs42:7.126L0 : ATTO FibreBridge6500N 1.61 FB6500N102974
   ```
Hot-swapping FibreBridge 6500N bridges to create a pair of FibreBridge 7600N or 7500N bridges

To hot-swap one or two FibreBridge 6500N bridges to create a configuration with a pair of FibreBridge 7600N or 7500N bridges, you must replace the bridges one at a time and follow the correct cabling procedure. The new cabling is different from the original cabling.

About this task

You can also use this procedure if the following conditions are true:

- You are replacing a pair of FibreBridge 6500N bridges that are both connected to the same stack of SAS storage.
- You previously replaced one FibreBridge 6500N bridge in the pair, and your storage stack is configured with one FibreBridge 6500N bridge and one FibreBridge 7600N or 7500N bridge. In this case, you should begin with Step 3 on page 44.

The following diagram shows an example of the initial configuration, in which four FibreBridge 6500N bridges are connecting two SAS storage stacks:
Steps

1. Using the following guidelines, hot-swap the “top” FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge using the procedure in Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge on page 33:

   - Connect the FibreBridge 7600N or 7500N bridge FC1 port to the switch or controller. This is the same connection that was made to the FibreBridge 6500N bridge FC1 port.
   - Do not connect the FibreBridge 7600N or 7500N bridge FC2 port at this time.

The following diagram shows that bridge_A_1a has been replaced and is now a FibreBridge 7600N or 7500N bridge:
2. Confirm connectivity to the bridge-connected disks and that the new FibreBridge 7500N is visible in the configuration:

```
run local sysconfig -v
```

**Example**

```
node_A_1> run local sysconfig -v
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA

slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>) Initiator port
  Firmware rev: 7.5.0
  Flash rev: 0.0.0
  Host Port Id: 0x60100
```
3. Using the following guidelines, hot-swap the “bottom” FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge using the procedure in Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge on page 33:

- Connect the FibreBridge 7600N or 7500N bridge FC2 port to the switch or controller. This is the same connection that was made to the FibreBridge 6500N bridge FC1 port.
- Do not connect the FibreBridge 7600N or 7500N bridge FC1 port at this time.
4. Confirm connectivity to the bridge-connected disks:

    run local sysconfig -v

The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

**Example**

```
node_A_1> run local sysconfig -v
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA

Configuration should be multi-path HA

slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)
  Firmware rev: 7.5.0
  Flash rev: 0.0.0
  Host Port Id: 0x60100
```
Cabling the bridge SAS ports when consolidating storage behind FibreBridge 7600N or 7500N bridges

When consolidating multiple SAS storage stacks behind a single pair of FibreBridge 7600N or 7500N bridges with available SAS ports, you must move the top and bottom SAS cables to the new bridges.

About this task

The FibreBridge 6500N bridge SAS ports use QSFP connectors. The FibreBridge 7600N or 7500N bridge SAS ports use mini-SAS connectors.

Attention: If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

Note: Wait at least 10 seconds before connecting the port. The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place and the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

Steps

1. Remove the cable that connects the SAS A port of the top FibreBridge 6500N bridge to the top SAS shelf, being sure to note the SAS port on the storage shelf to which it connects.

   The cable is shown in blue in the following example:
2. Using a cable with a mini-SAS connector, connect the same SAS port on the storage shelf to the SAS B port of the top FibreBridge 7600N or 7500N bridge. The cable is shown in blue in the following example:

3. Remove the cable that connects the SAS A port of the bottom FibreBridge 6500N bridge to the top SAS shelf, being sure to note the SAS port on the storage shelf to which it connects. This cable is shown in green in the following example:
4. Using a cable with a mini-SAS connector, connect the same SAS port on the storage shelf to the SAS B port of the bottom FibreBridge 7600N or 7500N bridge.

This cable is shown in green in the following example:

5. Confirm connectivity to the bridge-connected disks:
run local sysconfig -v

The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

Example

```
node_A_1> run local sysconfig -v
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA

--- Configuration should be multi-path HA

slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)
Firmware rev: 7.5.0
Flash rev: 0.0.0
Host Port Id: 0x60100
FC Node Name: 5:00a:098201:bae312
FC Port Name: 5:00a:098201:bae312
SFP Vendor: FINISAR CORP.
SFP Part Number: FTLF8529P3BCVAN1
SFP Serial Number: URQ0R1R
SFP Capabilities: 4, 8 or 16 Gbit
Link Data Rate: 16 Gbit
Switch Port: brcd6505-fcs40:1

List of disks visible to port
ID Vendor Model            FW    Size
brcd6505-fcs40:12.126L1527 : NETAPP   X302_HJUPI01TSSM NA04  847.5GB
(1953525168 512B/sect)
brcd6505-fcs40:12.126L1528 : NETAPP   X302_HJUPI01TSSA NA02  847.5GB
(1953525168 512B/sect)

List of FC-to-SAS bridges visible to port
FC-to-SAS Bridge:
brcd6505-fcs40:12.126L0 : ATTO FibreBridge7500N A30H FB7500N100104
brcd6505-fcs42:13.126L0 : ATTO FibreBridge7500N A30H FB7500N100104

List of storage shelves visible to port
brcd6505-fcs40:12.shelf8: DS4243 Firmware rev. IOM3 A: 0200 IOM3 B: 0200
```

6. Remove the old FibreBridge 6500N bridges that are no longer connected to the SAS storage.
7. Wait two minutes for the system to recognize the changes.
8. If the system was miscabled, remove the cable, correct the cabling, and then reconnect the correct cable.
9. If necessary, repeat the preceding steps to move up to two additional SAS stacks behind the new FibreBridge 7600N or 7500N bridges, using SAS ports C and then D.

Each SAS stack must be connected to the same SAS port on the top and bottom bridge. For example, if the top connection of the stack is connected to the top bridge SAS B port, the bottom connection must be connected to the SAS B port of the bottom bridge.
Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration

The zoning must be changed when you are replacing FibreBridge 6500N bridges with FibreBridge 7600N or 7500N bridges and using both FC ports on the FibreBridge 7600N or 7500N bridges. The required changes depend on whether you are running a version of ONTAP earlier than 9.1 or 9.1 and later.

**Choices**

- Updating zoning when adding FibreBridge 7500N bridges to a configuration (prior to ONTAP 9.1) on page 50
- Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration (ONTAP 9.1 and later) on page 54

**Updating zoning when adding FibreBridge 7500N bridges to a configuration (prior to ONTAP 9.1)**

The zoning must be changed when you are replacing FibreBridge 6500N bridges with FibreBridge 7500N bridges and using both FC ports on the FibreBridge 7500N bridges. Each zone can have no more than four initiator ports. The zoning you use depends on whether you are running ONTAP prior to version 9.1 or 9.1 and later

**About this task**

The specific zoning in this task is for versions of ONTAP prior to version 9.1.

The zoning changes are required to avoid issues with ONTAP, which requires that no more than four FC initiator ports can have a path to a disk. After recabling to consolidate the shelves, the existing zoning would result in each disk being reachable by eight FC ports. You must change the zoning to reduce the initiator ports in each zone to four.

The following diagram shows the zoning on site_A before the changes:
Performing FC-to-SAS bridge maintenance
Step

1. Update the storage zones for the FC switches by removing half of the initiator ports from each existing zone and creating new zones for the FibreBridge 7500N FC2 ports.

The zones for the new FC2 ports will contain the initiator ports removed from the existing zones. In the diagrams, these zones are shown with dashed lines.

For details about the zoning commands, see the FC switch sections of the Fabric-attached MetroCluster installation and configuration or Stretch MetroCluster installation and configuration.

Example

The following examples show the storage zones and the ports in each zone before and after the consolidation. The ports are identified by domain, port pairs.

- Domain 5 consists of switch FC_switch_A_1.
- Domain 6 consists of switch FC_switch_A_2.
- Domain 7 consists of switch FC_switch_B_1.
- Domain 8 consists of switch FC_switch_B_2.

<table>
<thead>
<tr>
<th>Before or after consolidation</th>
<th>Zone</th>
<th>Domains and ports</th>
<th>Colors in diagram*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zones before the consolidation.</td>
<td>STOR_A_1a-FC1</td>
<td>5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,6</td>
<td>Purple + dashed purple + blue</td>
</tr>
<tr>
<td>There is a zone for each FC port on the four FibreBridge 6500N bridges.</td>
<td>STOR_A_1b-FC1</td>
<td>6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,6</td>
<td>Brown + dashed brown + green</td>
</tr>
<tr>
<td>STOR_A_2a-FC1</td>
<td>5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,7</td>
<td>Purple + dashed purple + red</td>
<td></td>
</tr>
<tr>
<td>STOR_A_2b-FC1</td>
<td>6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,7</td>
<td>Brown + dashed brown + orange</td>
<td></td>
</tr>
<tr>
<td>Zones after the consolidation.</td>
<td>STOR_A_1a-FC1</td>
<td>7,1; 7,4; 5,1; 5,4; 5,6</td>
<td>Purple + blue</td>
</tr>
<tr>
<td>There is a zone for each FC port on the two FibreBridge 7500N bridges.</td>
<td>STOR_A_1b-FC1</td>
<td>7,2; 7,5; 5,2; 5,5; 5,7</td>
<td>Dashed purple + red</td>
</tr>
<tr>
<td>STOR_A_1a-FC2</td>
<td>8,1; 8,4; 6,1; 6,4; 6,6</td>
<td>Brown + green</td>
<td></td>
</tr>
<tr>
<td>STOR_A_1b-FC2</td>
<td>8,2; 8,5; 6,2; 6,5; 6,7</td>
<td>Dashed brown + orange</td>
<td></td>
</tr>
</tbody>
</table>

* The diagrams only show site_A.

The following diagram shows zoning at site_A after the consolidation:
Performing FC-to-SAS bridge maintenance
Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration (ONTAP 9.1 and later)

The zoning must be changed when you are replacing FibreBridge 6500N bridges with FibreBridge 7600N or 7500N bridges and using both FC ports on the FibreBridge 7600N or 7500N bridges. Each zone can have no more than four initiator ports.

About this task

• This task applies to ONTAP 9.1 and later.
• FibreBridge 7600N bridges are supported in ONTAP 9.6 and later.
• The specific zoning in this task is for ONTAP 9.1 and later.
• The zoning changes are required to avoid issues with ONTAP, which requires that no more than four FC initiator ports can have a path to a disk.

After recabling to consolidate the shelves, the existing zoning would result in each disk being reachable by eight FC ports. You must change the zoning to reduce the initiator ports in each zone to four.

Step

1. Update the storage zones for the FC switches by removing half of the initiator ports from each existing zone and creating new zones for the FibreBridge 7600N or 7500N FC2 ports. The zones for the new FC2 ports will contain the initiator ports removed from the existing zones.

The FC switch section of the Fabric-attached MetroCluster Installation and Configuration Guide contains details about the zoning commands.

Cabling the second bridge FC port when adding FibreBridge 7600N or 7500N bridges to a configuration

To provide multiple paths to the storage stacks, you can cable the second FC port on each FibreBridge 7600N or 7500N bridge when you have added the FibreBridge 7600N or 7500N bridge to your configuration.

Before you begin

The zoning must have been adjusted to provide zones for the second FC ports.

Steps

1. Cable the FC2 port of the top bridge to the correct port on FC_switch_A_2.
2. Cable the FC1 port of the bottom bridge to the correct port on FC_switch_A_1.
3. Confirm connectivity to the bridge-connected disks:

```
run local sysconfig -v
```

The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

**Example**

```
node_A_1> run local sysconfig -v
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA

slot 0: FC Host Adapter 0g [QLogic 8324 rev. 2, N-port, <UP>] Initiator port
Firmware rev: 7.5.0
Flash rev: 0.0.0
```
Disabling unused SAS ports on the FC-to-SAS bridges

After making cabling changes to the bridge, you should disable any unused SAS ports on FC-to-SAS bridges to avoid health monitor alerts related to the unused ports.

Steps

1. Disable unused SAS ports on the top FC-to-SAS bridge:
   
   a. Log in to the bridge CLI.
   
   b. Disable any unused ports.

   **Note:** If you have configured an ATTO 7500N bridge, then all of the SAS ports (A through D) are enabled by default, and you must disable the SAS ports that are not being used:

   ```
   SASPortDisable sas port
   ```

   **Example**

   If SAS ports A and B are used, then SAS ports C and D must be disabled. In the following example, the unused SAS ports C and D are disabled:

   ```
   Ready. *
   SASPortDisable C
   SAS Port C has been disabled.
   Ready. *
   SASPortDisable D
   SAS Port D has been disabled.
   Ready. *
   ```

   c. Save the bridge configuration:

   ```
   SaveConfiguration
   ```
Example

The following example shows that SAS ports C and D have been disabled. Note that the asterisk no longer appears, indicating that the configuration has been saved.

```
Ready. *
SaveConfiguration
Ready.
```

2. Repeat Step 1 on page 57 on the bottom FC-to-SAS bridge.

Requirements for using other interfaces to configure and manage FibreBridge bridges

You can use the combination of a serial port, Telnet, and FTP to manage the FibreBridge bridges instead of the recommended management interfaces. Your system must meet the requirements for the applicable interface before you install the bridges.

You can use a serial port or Telnet to configure the bridge and Ethernet management 1 port, and to manage the bridge. You can use FTP to update the bridge firmware.

**Note:** The *ATTO FibreBridge Installation and Operation Manual* for your model bridge has more information about management interfaces.

You can access this document on the ATTO web site by using the link provided on the ATTO Fibrebridge Description page.

*NetApp Downloads: ATTO FibreBridge 7600N*

*NetApp Downloads: ATTO FibreBridge 7500N*

*NetApp Downloads: ATTO FibreBridge 6500N*

Serial port

When using the serial port to configure and manage a bridge, and to configure the Ethernet management 1 port, your system must meet the following requirements:

- A serial cable (which connects from the bridge serial port to a serial (COM) port on the computer you are using for setup)
  The bridge serial port is RJ-45 and has the same pin-out as the controllers.

- A terminal emulation program such as Hyperterminal, Teraterm, or PuTTY to access the console
  The terminal program should be capable of logging screen output to a file.

Telnet

When using Telnet to configure and manage a bridge, your system must meet the following requirements:

- A serial cable (which connects from the bridge serial port to a serial (COM) port on the computer you are using for setup)
  The bridge serial port is RJ-45 and has the same pin-out as the controllers.

- (Recommended) A non-default user name and password (for accessing the bridge)

- A terminal emulation program such as Hyperterminal, Teraterm, or PuTTY to access the console
  The terminal program should be capable of logging screen output to a file.
• An IP address, subnet mask, and gateway information for the Ethernet management 1 port on each bridge

FTP

When using FTP to update bridge firmware, your system must meet the following requirements:

• A standard Ethernet cable (which connects from the bridge Ethernet management 1 port to your network)
• (Recommended) A non-default user name and password (for accessing the bridge)

Hot-replacing a failed power supply module

When there is a change in status of a power supply module to the bridge, you can remove and install the power supply module.

You can view the change in status of a power supply module through the LEDs on the bridge. You can also view the status of power supply modules via ExpressNAV GUI and the bridge CLI, via serial port, or via Telnet.

• This procedure is NDO (non-disruptive) and takes approximately 15 minutes to complete.
• You need the admin password and access to an FTP or SCP server.

Note: The ATTO FibreBridge Installation and Operation Manual for your model bridge has more information about management interfaces.

You can access this and other content on the ATTO web site by using the link provided on the ATTO Fibrebridge Description page.

NetApp Downloads: ATTO FibreBridge 7600N
NetApp Downloads: ATTO FibreBridge 7500N
NetApp Downloads: ATTO FibreBridge 6500N

In-band management of the FC-to-SAS bridges

Beginning with ONTAP 9.5 with FibreBridge 7500N or 7600N bridges, in-band management of the bridges is supported as an alternative to IP management of the bridges.

When using in-band management, the bridges can be managed and monitored from the ONTAP CLI via the FC connection to the bridge. Physical access to the bridge via the bridge Ethernet ports is not required, reducing the security vulnerability of the bridge.

Bridge CLI commands can be issued from the ONTAP interface storage bridge run-cli -name bridge-name -command bridge-command-name command at the ONTAP interface.

Note: Using in-band management with IP access disabled is recommended to improve security by limiting physical connectivity the bridge.

Related tasks

Hot-swapping a bridge with a replacement bridge of the same model on page 21
Hot-swapping a FibreBridge 7500N with a 7600N bridge on page 27
Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge on page 33
Hot-adding a stack of SAS disk shelves and bridges on page 106
Managing a FibreBridge bridge from ONTAP

Starting with ONTAP 9.5, you can use the ONTAP CLI to pass FibreBridge commands to the bridge and display the results of those commands.

Step

1. Run the applicable FibreBridge command within the `storage bridge run-cli` command:
   ```
   storage bridge run-cli -name bridge-name -command "command-text"
   ```

Example

The following command runs the FibreBridge `SASPortDisable` command from the ONTAP prompt to disable SAS port b on the bridge:

```
cluster_A::> storage bridge run-cli -name "SASPortDisable b"
SAS Port B has been disabled.
Ready
cluster_A::>
```

Securing or unsecuring the FibreBridge bridge

To easily disable potentially unsecure Ethernet protocols on a bridge, beginning with ONTAP 9.6 you can secure the bridge. This disables the bridge's Ethernet ports. You can also reenable Ethernet access.

About this task

- Securing the bridge disables telnet and other IP port protocols and services (FTP, ExpressNAV, ICMP, or QuickNAV) on the bridge.
- This procedure uses out-of-band management using the ONTAP prompt, which is available beginning with ONTAP 9.5.
- You can issue the commands from the bridge CLI if you are not using out-of-band management.
- The `unsecurebridge` command can be used to reenable the Ethernet ports.

Steps

1. From the ONTAP prompt of the cluster containing the bridge, secure or unsecure the bridge.

Example

The following command secures `bridge_A_1`:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
```

The following command unsecures `bridge_A_1`:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
```

2. From the ONTAP prompt of the cluster containing the bridge, save the bridge configuration:
   `storage bridge run-cli -bridge bridge-name -command saveconfiguration`
Example
The following command secures bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command savemodification
```

3. From the ONTAP prompt of the cluster containing the bridge, restart the bridge's firmware:

```
storage bridge run-cli -bridge bridge-name -command firmwarerestart
```

Example
The following command secures bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
```
Performing FC switch maintenance and replacement

If necessary, you can non-disruptively replace the FC switches or upgrade their firmware in the MetroCluster configuration.

Choices

- Upgrading or downgrading the firmware on a Brocade FC switch on page 62
- Upgrading or downgrading the firmware on a Cisco FC switch on page 65
- Upgrading to new Brocade FC switches on page 67
- Replacing a Brocade FC switch on page 71
- Renaming a Brocade FC switch on page 75
- Changing ISL properties, ISL ports, or the IOD/OOD configuration on a Brocade switch on page 77
- Replacing a Cisco FC switch on page 81
- Changing speed of ISL ports on a Cisco FC switch on page 88
- Adding ISLs to a Cisco switch on page 89

Upgrading or downgrading the firmware on a Brocade FC switch

To upgrade or downgrade the firmware on a Brocade FC switch, you must use the Brocade-specific commands to disable the switch, perform and verify the firmware change, and reboot and reenable the switch.

Before you begin

- You must have the firmware files.
- The system must be properly cabled.
- All paths to the storage shelves must be available.
- The disk shelf stacks must be stable.
- The FC switch fabric must be healthy.
- No failed components can be present in the system.
- The system must be operating normally.
- You must have the admin password and access to an FTP or SCP server.

About this task

The switch fabric is disabled during a firmware upgrade or downgrade, and the MetroCluster configuration relies on the second fabric to continue operation.

This task must be performed on each of the switch fabrics in succession so that all switches are running the same firmware version.

Note: This procedure is nondisruptive and takes approximately one hour to complete.
Steps

1. Log in to each of the switches in the fabric.
   The examples in the following steps use the switch `FC_switch_A_1`.

2. Disable each of the switches in the fabric:
   
   ```
   switchCfgPersistentDisable
   ```

   If this command is not available, then run the `switchDisable` command.

   Example

   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

3. Download the desired firmware version:

   ```
   firmwareDownload
   ```

   When prompted for the file name, you must specify the subdirectory or relative path to the firmware file.

   You can run the `firmwareDownload` command at the same time on both switches, but you must allow the firmware to download and commit properly before moving to the next step.

   Example

   ```
   FC_switch_A_1:admin> firmwaredownload
   Server Name or IP Address: 10.64.203.188
   User Name: test
   File Name: v7.3.1b
   Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
   Password: 
   Server IP: 10.64.203.188, Protocol IPv4
   Checking system settings for firmwaredownload...
   System settings check passed.
   ```

4. Verify that the firmware was downloaded and committed to both partitions:

   ```
   firmwareShow
   ```

   Example

   ```
   FC_switch_A_1:admin> firmwareShow
   Appl  Primary/Secondary Versions
   -------------------------------
   FOS     v7.3.1b
           v7.3.1b
   ```

5. Reboot the switches:

   ```
   reboot
   ```

   Some firmware versions automatically perform an haReboot operation after the firmware download is finished. The reboot in this step is required even if the haReboot has been performed.

   Example

   ```
   FC_switch_A_1:admin> reboot
   ```
6. Check whether the new firmware is for an intermediate firmware level or for a final specified release.

   If the download is for the intermediate firmware level, then perform the previous two steps until the specified release is installed.

7. Enable the switches:

   `switchCfgPersistentEnable`

   If this command is not available, then the switch should be in the enabled state after the `reboot` command is executed.

   **Example**

   ```
   FC_switch_A_1:admin> switchCfgPersistentEnable
   ```

8. Verify that the switches are online and that all of the devices are properly logged in:

   `switchShow`

   **Example**

   ```
   FC_switch_A_1:admin> switchShow
   ```

9. Verify that the buffer usage information for a port group or all of the port groups in the switch is displayed properly:

   `portbuffershow`

   **Example**

   ```
   FC_switch_A_1:admin> portbuffershow
   ```

10. Verify that the current configuration of a port is displayed properly:

    `portcfgshow`

    **Example**

    ```
    FC_switch_A_1:admin> portcfgshow
    ```

    Verify the port settings, such as speed, mode, trunking, encryption, and compression, in the Inter-Switch Link (ISL) output. Verify that the port settings were not affected by the firmware download.

11. 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:
Performing FC switch maintenance and replacement | 65

metrocluster check show

f. Run Config Advisor.

NetApp Downloads: Config Advisor

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

12. Repeat this procedure for the second switch fabric.

Upgrading or downgrading the firmware on a Cisco FC switch

To upgrade or downgrade the firmware on a Cisco FC switch you must use the Cisco-specific commands to disable the switch, perform and verify the upgrade, and reboot and reenable the switch.

Before you begin

• The system must be properly cabled.
• All paths to the storage shelves must be available.
• The disk shelf stacks must be stable.
• The FC switch fabric must be healthy.
• All components in the system must be healthy.
• The system must be operating normally.
• You need the admin password and access to an FTP or SCP server.

About this task

The switch fabric is disabled during the firmware upgrade or downgrade and the MetroCluster configuration relies on the second fabric to continue operation.

You must repeat this task on each of the switch fabrics in succession to ensure that all switches are running the same firmware version.

You must have the firmware files.

Note: This procedure is nondisruptive and takes approximately one hour to complete.

Steps

1. Log in to each of the switches in the fabric.
   In the examples, the switches are called FC_switch_A_1 and FC_switch_B_1.

2. Determine whether there is enough space in the bootflash directory on each switch:
   dir bootflash
   If not, delete the unwanted firmware files by using the delete bootflash:file_name command.

3. Copy the kickstart and system files to the switches:
   copy source_file target_file
Example
In the following example, the kickstart file (m9200-s2ek9-kickstart-mz.5.2.1.bin) and the system file (m9200-s2ek9-mz.5.2.1.bin) are located on the FTP server 10.10.10.55 in the /firmware/ path.

The following example shows the commands issued on FC_switch_A_1:

```
FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-kickstart-mz.5.2.1.bin bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-mz.5.2.1.bin bootflash:m9200-s2ek9-mz.5.2.1.bin
```

4. Disable all the VSANs on both the switches in this fabric.

5. Install the desired firmware on the switches:

```
install all system bootflash:systemfile_name kickstart bootflash:kickstartfile_name
```

Example
The following example shows the commands issued on FC_switch_A_1:

```
FC_switch_A_1# install all system bootflash:m9200-s2ek9-mz.5.2.1.bin kickstart bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
Enter Yes to confirm the installation.
```

6. Check the version of the firmware on each switch to make sure the correct version was installed:

```
show version
```

7. Enable all the VSANs on both the switches in this fabric.

8. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:

```
node run -node (node name) sysconfig -a
```
   b. Check for any health alerts on both clusters:

```
system health alert show
```
   c. Confirm the MetroCluster configuration and that the operational mode is normal:

```
metrocluster show
```
   d. Perform a MetroCluster check:

```
metrocluster check run
```
   e. Display the results of the MetroCluster check:

```
metrocluster check show
```
   f. Run Config Advisor.

   NetApp Downloads: Config Advisor

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

9. Repeat this procedure for the second switch fabric.
Upgrading to new Brocade FC switches

If you are upgrading to new Brocade FC switches, you must replace the switches in the first fabric, verify that the MetroCluster configuration is fully operational, and then replace the switches in the second fabric.

Before you begin

- The MetroCluster configuration must be healthy and in normal operation.
- The MetroCluster switch fabrics consist of four Brocade switches. The illustrations in the following steps show current switches.
- The switches must be running the most recent supported firmware.

NetApp Interoperability Matrix Tool

About this task

- This procedure is nondisruptive and takes approximately two hours to complete.
- You need the admin password and access to an FTP or SCP server.

The switch fabrics are upgraded one at a time.

At the end of this procedure, all four switches will be upgraded to new switches.

Steps

1. Disable the first switch fabric:

   FC_switch_A_1:admin> switchCfgPersistentDisable
2. Replace the old switches at one MetroCluster site.
   a. Uncable and remove the disabled switch.
   b. Install the new switch in the rack.
c. Disable the new switches:

\texttt{switchCfgPersistentDisable}

The command disables both switches in the switch fabric.

\texttt{FC_switch_A_1:admin> switchCfgPersistentDisable}

d. Cable the new switch using the recommended port assignments.

\textit{Port assignments for FC switches when using ONTAP 9.0} on page 210

\textit{Port assignments for FC switches when using ONTAP 9.1 and later} on page 224

e. Repeat these substeps at the partner MetroCluster site to replace the second switch in the first switch fabric.

Both switches in fabric 1 have been replaced.

3. Power up the new switches and let them boot up.

4. Download the RCF files for the new switch.

\textit{NetApp Downloads: MetroCluster Configuration Files for Brocade Switches}

5. Apply the RCF files to both new switches in the fabric, following the directions on the download page.

6. Save the switch configuration:

\texttt{cfgSave}

7. Wait 10 minutes to allow the configuration to stabilize.

8. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:
run local sysconfig -v

The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

Example

```bash
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA

slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)
  Firmware rev: 7.5.0
  Host Port Id: 0x60130
  FC Node Name: 5:00a:098201:bae312
  FC Port Name: 5:00a:098201:bae312
  SFP Vendor: UTILITIES CORP.
  SFP Part Number: FTLE8529P3BCVAN1
  SFP Serial Number: URQ0Q9R
  SFP Capabilities: 4, 8 or 16 Gbit
  Link Data Rate: 16 Gbit
  Switch Port: brcd6505-fcs40:1
  List of disks visible to port
  ID Vendor Model            FW    Size
  brcd6505-fcs29:12.126L1527 : NETAPP   X302_HJUPI01TSSM NA04 847.5GB
   (1953525168 512B/sect)
  brcd6505-fcs29:12.126L1528 : NETAPP   X302_HJUPI01TSSA NA02 847.5GB
   (1953525168 512B/sect)

<List of FC-to-SAS bridges visible to port>
FC-to-SAS Bridge:
  brcd6505-fcs40:12.126L0 : ATTO FibreBridge6500N 1.61  FB6500N102980
  brcd6505-fcs42:13.126L0 : ATTO FibreBridge6500N 1.61  FB6500N102980
  brcd6505-fcs42:6.126L0 : ATTO FibreBridge6500N 1.61  FB6500N101167
  brcd6505-fcs42:7.126L0 : ATTO FibreBridge6500N 1.61  FB6500N102974

<List of storage shelves visible to port>
  brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200 IOM3 B: 0200
```

9. Returning to the switch prompt, verify the switch firmware version:

```bash
firmwareShow
```

The switches must be running the most recent supported firmware.

*NetApp Interoperability Matrix Tool*

10. Simulate a switchover operation:

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

```bash
set -privilege advanced
```

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

b. Perform the switchover operation with the `-simulate` parameter:

```bash
metrocluster switchover -simulate
```

c. Return to the admin privilege level:

```bash
set -privilege admin
```

11. Repeat the previous steps on the second switch fabric.
Replacing a Brocade FC switch

You must use this Brocade-specific procedure to replace a failed switch.

Before you begin

You need the admin password and access to an FTP or SCP server.

About this task

In the following examples, FC_switch_A_1 is the healthy switch and FC_switch_B_1 is the impaired switch. The switch port usage in the examples is shown in the following table:

<table>
<thead>
<tr>
<th>Port connections</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-VI connections</td>
<td>0, 3</td>
</tr>
<tr>
<td>HBA connections</td>
<td>1, 2, 4, 5</td>
</tr>
<tr>
<td>FC-to-SAS bridge connections</td>
<td>6, 7</td>
</tr>
<tr>
<td>ISL connections</td>
<td>10, 11</td>
</tr>
</tbody>
</table>

The examples show two FC-to-SAS bridges. If you have more, you must disable and subsequently enable the additional ports.

Note: This procedure is nondisruptive and takes approximately two hours to complete.

Your switch port usage should follow the recommended assignments.

•  Port assignments for FC switches when using ONTAP 9.0 on page 210
Steps

1. Fence off the switch undergoing replacement by disabling the ISL ports on the healthy switch in the fabric and the FC-VI and HBA ports on the impaired switch (if the impaired switch is still operating):
   a. Disable the ISL ports on the healthy switch for each port:

   ```
   portcfgpersistentdisable port-number
   ```

   Example

   ```
   FC_switch_A_1:admin> portcfgpersistentdisable 10
   FC_switch_A_1:admin> portcfgpersistentdisable 11
   ```

   b. If the impaired switch is still operational, disable the FC-VI and HBA ports on that switch for each port:

   ```
   portcfgpersistentdisable port-number
   ```

   Example

   ```
   FC_switch_B_1:admin> portcfgpersistentdisable 0
   FC_switch_B_1:admin> portcfgpersistentdisable 1
   FC_switch_B_1:admin> portcfgpersistentdisable 2
   FC_switch_B_1:admin> portcfgpersistentdisable 3
   FC_switch_B_1:admin> portcfgpersistentdisable 4
   FC_switch_B_1:admin> portcfgpersistentdisable 5
   ```

2. If the impaired switch is still operational, gather the output from the `switchshow` command.

   Example

   ```
   FC_switch_B_1:admin> switchshow
   switchName: FC_switch_B_1
   switchType: 71.2
   switchState:Online
   switchMode: Native
   switchRole: Subordinate
   switchDomain: 2
   switchId: fffc01
   switchWwn: 10:00:00:05:33:86:89:cb
   zoning: OFF
   switchBeacon: OFF
   ```

3. Boot and preconfigure the new switch prior to physically installing it:
   a. Power up the new switch and let it boot up.
   b. Check the firmware version on the switch to confirm that it matches the version of the other FC switches:

   ```
   firmwareShow
   ```

   c. Configure the new switch as described in the `MetroCluster Installation and Configuration Guide`, but skipping the “Configuring zoning on Brocade FC switches” section.

   ```
   Fabric-attached MetroCluster installation and configuration
   ```

   You configure zoning later in this procedure.
Note: At this point, the new switch is not cabled to the MetroCluster configuration.

d. Disable the FC-VI, HBA, and storage ports on the new switch, and the ports connected to the FC-SAS bridges.

Example

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5
FC_switch_B_1:admin> portcfgpersistentdisable 6
FC_switch_B_1:admin> portcfgpersistentdisable 7
```

4. Physically replace the switch:

   a. Power off the impaired FC switch.

   b. Power off the replacement FC switch.

   c. Uncable and remove the impaired switch, carefully noting which cables connected to which ports.

   d. Install the replacement switch in the rack.

   e. Cable the replacement switch exactly as the old switch was cabled.

   f. Power on the new FC switch.

5. If you want to enable ISL encryption, complete the applicable tasks in the Fabric-attached MetroCluster Installation and Configuration Guide.

   If you are enabling ISL encryption, you need to complete the following tasks:

   • Disabling the virtual fabric

   • Setting the payload

   • Setting the authentication policy

   • Enabling ISL encryption on Brocade switches

6. Complete the configuration of the new switch:

   a. Enable the ISLs:

      ```
      portcfgpersistentenable port-number
      ```

      Example

      ```
      FC_switch_B_1:admin> portcfgpersistentenable 10
      FC_switch_B_1:admin> portcfgpersistentenable 11
      ```

   b. On the replacement switch (FC_switch_B_1 in the example), verify that the ISLs are online:

      ```
      switchshow
      ```
**Example**

```
FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 71.2
switchState: Online
switchMode: Native
switchRole: Principal
switchDomain: 4
switchId: fffe03
switchWwn: 10:00:00:05:33:8c:2e:9a
zoning: OFF
switchBeacon: OFF
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Port</th>
<th>Address</th>
<th>Media</th>
<th>Speed</th>
<th>State</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>030A00</td>
<td>id</td>
<td>16G</td>
<td>Online</td>
<td>FC E-Port</td>
</tr>
<tr>
<td>10:00:00:05:33:8c:2e:9a &quot;FC_switch_A_1&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>030B00</td>
<td>id</td>
<td>16G</td>
<td>Online</td>
<td>FC E-Port</td>
</tr>
<tr>
<td>10:00:00:05:33:8e:89:cb &quot;FC_switch_A_1&quot; (downstream)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**c. Enable the storage ports that connect to the FC bridges.**

**Example**

```
FC_switch_B_1:admin> portcfgpersistentenable 6
FC_switch_B_1:admin> portcfgpersistentenable 7
```

**d. Enable the storage, HBA, and FC-VI ports.**

**Example**

The following example shows the commands used to enable the ports connecting HBA adapters:

```
FC_switch_B_1:admin> portcfgpersistentenable 1
FC_switch_B_1:admin> portcfgpersistentenable 2
FC_switch_B_1:admin> portcfgpersistentenable 4
FC_switch_B_1:admin> portcfgpersistentenable 5
```

The following example shows the commands used to enable the ports connecting the FC-VI adapters:

```
FC_switch_B_1:admin> portcfgpersistentenable 0
FC_switch_B_1:admin> portcfgpersistentenable 3
```

**7. Verify that the ports are online:**

`switchshow`

**8. 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:

   \texttt{metrocluster check run}

e. Display the results of the MetroCluster check:

   \texttt{metrocluster check show}

f. Run Config Advisor.

   \textit{NetApp Downloads: Config Advisor}

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

### Renaming a Brocade FC switch

You might need to rename a Brocade FC switch to ensure consistent naming throughout your configuration.

**Steps**

1. Persistently disable the switch or switches in one fabric: \texttt{switchcfgpersistentdisable}

   The following example shows the output for the \texttt{switchcfgpersistentdisable} command:

   **Example**

   ```bash
   7840.FCIP_2:admin> switchcfgpersistentdisable
   Switch's persistent state set to 'disabled'
   2018/03/09-07:41:06, [ESM-2105], 146080, FID 128, INFO, 7840.FCIP_2, VE Tunnel 24 is DEGRADED.
   2018/03/09-07:41:06, [ESM-2104], 146081, FID 128, INFO, 7840.FCIP_2, VE Tunnel 24 is OFFLINE.
   7840.FCIP_2:admin>
   ```

2. Rename the switch or switches: \texttt{switchname new-switch-name}

   If you are renaming both switches in the fabric, use the same command on each switch.

   The following example shows the output for the \texttt{switchname new-switch-name} command:

   **Example**

   ```bash
   7840.FCIP_2:admin> switchname FC_switch_1_B
   Committing configuration...
   Done.
   Switch name has been changed. Please re-login into the switch for the change to be applied.
   2018/03/09-07:41:20, [IPAD-1002], 146082, FID 128, INFO, FC_switch_1_B, Switch name has been successfully changed to FC_switch_1_B.
   7840.FCIP_2:admin>
   ```

3. Reboot the switch or switches: \texttt{reboot}

   If you are renaming both switches in the fabric, reboot both switches. Once the reboot is complete, the switch is renamed in all places.

   The following example shows the output for the \texttt{reboot} command:

   **Example**

   ```bash
   7840.FCIP_2:admin> reboot
   Warning: This command would cause the switch to reboot and result in traffic disruption.
   Are you sure you want to reboot the switch [y/n]? y
   2018/03/09-07:42:08, [RAS-1007], 146083, CHASSIS, INFO, Brocade7840, System is about to reload.
   Rebooting! Fri Mar  9 07:42:11 CET 2018
   ```
4. Persistently enable the switches: `switchcfgpersistentenable`  

The following example shows the output for the `switchcfgpersistentenable` command:

**Example**

```
FC_switch_1_B:admin> switchcfgpersistentenable
Switch’s persistent state set to 'enabled'
FC_switch_1_B:admin> FC_switch_1_B:admin> FC_switch_1_B:admin>
FC_switch_1_B:admin> 2018/03/09-08:07:07, [ESM-2105], 146106, FID 128, INFO, FC_switch_1_B, VE Tunnel 24 is DEGRADED.
2018/03/09-08:07:10, [ESM-2106], 146107, FID 128, INFO, FC_switch_1_B, VE Tunnel 24 is ONLINE.
FC_switch_1_B:admin>
FC_switch_1_B:admin> switchshow
switchName:     FC_switch_1_B
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   6
switchId:       fffc06
switchWwn:      10:00:50:eb:1a:9a:a5:79
zoning:         ON (CFG_FAB_2_RCF_9_3)
switchBeacon:   OFF
FC Router:      OFF
FC Router BB Fabric ID: 128
Address Mode:   0
HIF Mode:       OFF

Index Port Address Media Speed   State       Proto
==================================================
0   0   060000   id    16G     Online      FC  F-Port  50:0a:09:81:06:a5:5a:08
1   1   060100   id    16G     Online      FC  F-Port  50:0a:09:83:06:a5:5a:08
```

5. Verify that the switch name change is visible from the ONTAP cluster prompt: `storage switch show`  

The following example shows the output for the `storage switch show` command:

**Example**

```
cluster_A::*> storage switch show
(storage switch show)
Symbolic Name                  Vendor         Model               Switch WWN       Is Monitored Status
--------------------------------------------------------------------------------------------------------
Brocade_172.20.7.90             RTP-FC01-510Q40 Brocade Brocade7840 1000c4f57c904bc8 true ok
Brocade_172.20.7.91             RTP-FC02-510Q40 Brocade Brocade7840 100050eb1a9aa579 true ok
Brocade_172.20.7.92
```
Changing ISL properties, ISL ports, or the IOD/OOD configuration on a Brocade switch

You might need to add ISLs to a switch if you are adding or upgrading hardware such as additional or faster controllers or switches.

Before you begin

Ensure that the system is properly configured, that all fabric switches are operational, and that no errors exist.

About this task

If the equipment on the ISL link changes and the new link configuration no longer supports the current configuration—trunking and ordered delivery—then the fabric needs to be reconfigured for the correct routing policy: either in-order-deliver (IOD) or out-of-order-delivery (OOD).

Steps

1. Disable the FCVI and storage HBA ports: `portcfgpersistentdisable port number`

   By default the first 8 ports (ports 0 through 7) are used for FCVI and Storage HBA. The ports must be persistently disabled so that the ports remain disabled in the event of a switch reboot.

   Example

   The following example shows ISL ports 0–7 being disabled on both switches:

   ```
   Switch_A_1:admin> portcfgpersistentdisable 0-7
   Switch_B_1:admin> portcfgpersistentdisable 0-7
   ```

2. Change the ISL ports as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>To change the speed of an ISL port...</td>
<td>Use the <code>portcfgspeed port number port speed</code> command on both switches on the fabric. In the following example, you change the ISL port speed from 40 Gbps to 16 Gbps: <code>brocade_switch_A_1:admin&gt; portcfgspeed 40 16</code> You can verify that the speed has changed using the <code>switchshow</code> command: <code>brocade_switch_A_1:admin&gt; switchshow</code> You should see the following output:</td>
</tr>
<tr>
<td></td>
<td>. . . 40 40 062800 1d 16G No_Sync FC Disabled</td>
</tr>
<tr>
<td>To change the distance of an ISL port...</td>
<td>Use the <code>portcfglongdistance port number port distance</code> command on both switches in the fabric.</td>
</tr>
<tr>
<td>To remove an ISL...</td>
<td>Disconnect the link (cable).</td>
</tr>
<tr>
<td>To add an ISL...</td>
<td>Insert SFPs into the ports you are adding as ISL ports. Ensure that these ports are listed in the Fabric-attached MetroCluster Installation and Configuration Guide for the switch you are adding them to and cable them according to this guide.</td>
</tr>
</tbody>
</table>
To relocate an ISL...

Relocating an ISL is the same as removing and then adding an ISL. First, remove the ISL by disconnecting the link and then insert SFPs into the ports you are adding as ISL ports.

3. Reconfigure for out-of-order delivery (OOD) or in-order-delivery (IOD).

**Note:** If the routing policies remain the same, you do not need to reconfigure and this step can be ignored. The ONTAP configuration needs to match the fabric configuration. If the fabric is configured for OOD, then ONTAP must also be configured for OOD. The same applies for IOD.

This step should be executed in the following scenarios:

- More than one ISL formed a trunk before the change, but after the change, trunking is no longer supported. In this case, you must configure the fabric for OOD.
- There is one ISL before the change and multiple ISLs after the change.
  - If multiple ISLs form a trunk, configure the fabric for IOD.
  - If multiple ISLs **cannot** form a trunk, configure the fabric for OOD.

a. Persistently disable the switches using the `switchcfgpersistentdisable` command as shown in the following example:

**Example**

```
Switch_A_1:admin> switchcfgpersistentdisable
Switch_B_1:admin> switchcfgpersistentdisable
```

b. Configure the trunking mode for each ISL `portcfgtrunkport port number` as shown in the following table:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the ISL for trunking (IOD)</td>
<td>Set the <code>portcfgtrunkport port number</code> to 1:</td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_A_1:admin&gt; portcfgtrunkport 20 1</code></td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_A_1:admin&gt; portcfgtrunkport 21 1</code></td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_B_1:admin&gt; portcfgtrunkport 20 1</code></td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_B_1:admin&gt; portcfgtrunkport 21 1</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure the ISL for trunking (OOD)</th>
<th>Set the <code>portcfgtrunkport port number</code> to 0:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>FC_switch_A_1:admin&gt; portcfgtrunkport 20 0</code></td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_A_1:admin&gt; portcfgtrunkport 21 0</code></td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_B_1:admin&gt; portcfgtrunkport 20 0</code></td>
</tr>
<tr>
<td></td>
<td><code>FC_switch_B_1:admin&gt; portcfgtrunkport 21 0</code></td>
</tr>
</tbody>
</table>

c. Configure the fabric for IOD or OOD as required.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the fabric for IOD</td>
<td>Set the three settings of IOD, APT, and DLS using the <strong>iodset</strong>, <strong>aptpolicy</strong>, and <strong>dlsreset</strong> commands as shown in the following example:</td>
</tr>
</tbody>
</table>
|                          |Switch_A_1:admin> iodset  
|                          |Switch_A_1:admin> aptpolicy 1  
|                          |Policy updated successfully.  
|                          |Switch_A_1:admin> dlsreset  
|                          |FC_switch_A_1:admin> portcfgtrunkport  
|                          |40 1  
|                          |FC_switch_A_1:admin> portcfgtrunkport  
|                          |41 1  
|                          |Switch_B_1:admin> iodset  
|                          |Switch_B_1:admin> aptpolicy 1  
|                          |Policy updated successfully.  
|                          |Switch_B_1:admin> dlsreset  
|                          |FC_switch_B_1:admin> portcfgtrunkport  
|                          |20 1  
|                          |FC_switch_B_1:admin> portcfgtrunkport  
|                          |21 1  |
| Configure the fabric for OOD | Set the three settings of IOD, APT, and DLS using the **iodreset**, **aptpolicy**, and **dlsset** commands as shown in the following example: |
|                          |Switch_A_1:admin> iodreset  
|                          |Switch_A_1:admin> aptpolicy 3  
|                          |Policy updated successfully.  
|                          |Switch_A_1:admin> dlsset  
|                          |FC_switch_A_1:admin> portcfgtrunkport  
|                          |40 0  
|                          |FC_switch_A_1:admin> portcfgtrunkport  
|                          |41 0  
|                          |Switch_B_1:admin> iodreset  
|                          |Switch_B_1:admin> aptpolicy 3  
|                          |Policy updated successfully.  
|                          |Switch_B_1:admin> dlsset  
|                          |FC_switch_B_1:admin> portcfgtrunkport  
|                          |40 0  
|                          |FC_switch_B_1:admin> portcfgtrunkport  
|                          |41 0  |

**d.** Enable the switches persistently using the **switchcfgpersistentenable** command.

**Example**

```
switch_A_1:admin> switchcfgpersistentenable  
switch_B_1:admin> switchcfgpersistentenable
```

If this command does not exist, use the **switchenable** command as shown in the following example:

**Example**

```
brocade_switch_A_1:admin> switchenable  
```

**e.** Verify the OOD settings using the **iodshow**, **aptpolicy**, and **dlsshow** commands as shown in the following example:
Example

```
switch_A_1:admin> iodshow
IOD is not set
switch_A_1:admin> aptpolicy
Current Policy: 3 0(ap)
  3 0(ap) : Default Policy
  1: Port Based Routing Policy
  3: Exchange Based Routing Policy
  0: AP Shared Link Policy
  1: AP Dedicated Link Policy
command aptpolicy completed
switch_A_1:admin> dlsshow
DLS is set by default with current routing policy
```

Note: You must run these commands on both switches.

f. Verify the IOD settings using the `iodshow`, `aptpolicy`, and `dlsshow` commands as shown in the following example:

Example

```
switch_A_1:admin> iodshow
IOD is set
switch_A_1:admin> aptpolicy
Current Policy: 1 0(ap)
  3 0(ap) : Default Policy
  1: Port Based Routing Policy
  3: Exchange Based Routing Policy
  0: AP Shared Link Policy
  1: AP Dedicated Link Policy
command aptpolicy completed
switch_A_1:admin> dlsshow
DLS is not set
```

Note: You must run these commands on both switches.

4. Verify that the ISLs are online and trunked (if the linking equipment supports trunking) using the `islshow` and `trunkshow` commands.

   Note: If FEC is enabled, the deskew value of the last online port of the trunk group might show a difference of up to 36 although the cables are all of the same length.

<table>
<thead>
<tr>
<th>Are ISLs trunked?</th>
<th>You see the following system output...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>If the ISLs are trunked, only a single ISL appears in the output for the <code>islshow</code> command. Either port 40 or 41 can appear depending on which is the trunk master. The output of <code>trunkshow</code> should one trunk with ID ‘1’ listing both the physical ISLs on ports 40 and 41. In the following example the ports 40 and 41 are configured for use as an ISL:</td>
</tr>
</tbody>
</table>

```
switch_A_1:admin> islshow 1:
40-> 40 10:00:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw:
32.000G TRUNK CR_RECOV FEC
switch_A_1:admin> trunkshow
1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER
41-> 41 10:00:00:05:33:88:9c:68 2 deskew 15
```
Are ISLs trunked?  

<table>
<thead>
<tr>
<th>No</th>
<th>You see the following system output...</th>
</tr>
</thead>
</table>

If the ISLs are not trunked, both ISLs appear separately in the outputs for `islshow` and `trunkshow`. Both commands list the ISLs with their ID of ‘1’ and ‘2’. In the following example, the ports 40 and 41 are configured for use as an ISL:

```bash
switch_A_1:admin> islshow
1: 40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC
2: 41-> 41 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC

switch_A_1:admin> trunkshow
1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER
2: 41-> 41 10:00:00:05:33:88:9c:68 2 deskew 48 MASTER
```

5. Run the `spinfab` command on both switches to verify that the ISLs are healthy:

Example

```bash
switch_A_1:admin> spinfab -ports 0/40 - 0/41
```

6. Enable the ports that were disabled in step 1: `portenable port number`

Example

The following example shows ISL ports 0–7 being enabled:

```bash
brocade_switch_A_1:admin> portenable 0-7
```

### Replacing a Cisco FC switch

You must use Cisco-specific steps to replace a failed Cisco FC switch.

**Before you begin**

You need the admin password and access to an FTP or SCP server.

**About this task**

This procedure is nondisruptive and takes approximately two hours to complete.

In the examples in this procedure, `FC_switch_A_1` is the healthy switch and `FC_switch_B_1` is the impaired switch. The switch port usage in the examples is shown in the following table:

<table>
<thead>
<tr>
<th>Role</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-VI connections</td>
<td>1, 4</td>
</tr>
<tr>
<td>HBA connections</td>
<td>2, 3, 5, 6</td>
</tr>
<tr>
<td>FC-to-SAS bridge connections</td>
<td>7, 8</td>
</tr>
<tr>
<td>ISL connections</td>
<td>36, 40</td>
</tr>
</tbody>
</table>

The examples show two FC-to-SAS bridges. If you have more, you must disable and subsequently enable the additional ports.

Your switch port usage should follow the recommended assignments.

- *Port assignments for FC switches when using ONTAP 9.0* on page 210
- *Port assignments for FC switches when using ONTAP 9.1 and later* on page 224
Steps

1. Disable the ISL ports on the healthy switch to fence off the impaired switch.
   These steps are performed on the healthy switch.
   a. Enter configuration mode:
      ```conf t```
   b. Disable the ISL ports on the healthy switch with the `interface` and `shut` commands.
      ```
      FC_switch_A_1# conf t
      FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config)# shut
      FC_switch_A_1(config)# interface fc1/40
      FC_switch_A_1(config)# shut
      ```
   c. Exit configuration mode and copy the configuration to the startup configuration.
      ```
      FC_switch_A_1(config)# end
      FC_switch_A_1# copy running-config startup-config
      FC_switch_A_1#
      ```

2. Fence off the FC-VI and HBA ports on the impaired switch (if it is still running).
   These steps are performed on the impaired switch.
   a. Enter configuration mode:
      ```conf t```
   b. If the impaired switch is still operational, disable the FC-VI and HBA ports on the impaired switch with the `interface` and `shut` commands.
      ```
      FC_switch_B_1(config)# interface fc1/1
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/4
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/2-3
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/5-6
      FC_switch_B_1(config)# shut
      ```
   c. Exit configuration mode and copy the configuration to the startup configuration.
      ```
      FC_switch_B_1(config)# end
      FC_switch_B_1# copy running-config startup-config
      FC_switch_B_1#
      ```

3. If the impaired switch is still operational, determine the WWN for the switch:
   ```show wwn switch```
4. Boot and preconfigure the replacement switch, prior to physically installing it.

At this point the replacement switch is not cabled to the MetroCluster configuration. The ISL ports on the partner switch are disabled (in shut mode) and offline.

a. Power on the replacement switch and let it boot up.

b. Check the firmware version on the replacement switch to confirm that it matches the version of the other FC switches:

   ```
   show version
   ```

c. Configure the replacement switch as described in the *MetroCluster Installation and Configuration Guide*, skipping the “Configuring zoning on a Cisco FC switch” section.

   *Fabric-attached MetroCluster installation and configuration*

   You will configure zoning later in this procedure.

d. Disable the FC-VI, HBA, and storage ports on the replacement switch.

   ```
   FC_switch_B_1# conf t
   FC_switch_B_1(config)# interface fc1/1
   FC_switch_B_1(config)# shut
   FC_switch_B_1(config)# interface fc1/4
   FC_switch_B_1(config)# shut
   FC_switch_B_1(config)# interface fc1/2-3
   FC_switch_B_1(config)# shut
   FC_switch_B_1(config)# interface fc1/5-6
   FC_switch_B_1(config)# shut
   FC_switch_B_1(config)# interface fc1/7-8
   FC_switch_B_1(config)# shut
   FC_switch_B_1# copy running-config startup-config
   FC_switch_B_1#
   ```

5. Physically replace the impaired switch:

a. Power off the impaired switch.

b. Power off the replacement switch.

c. Uncable and remove the impaired switch, carefully noting which cables connected to which ports.

d. Install the replacement switch in the rack.

e. Cable the replacement switch exactly as the impaired switch was cabled.

f. Power on the replacement switch.

6. Enable the ISL ports on the replacement switch.
Example

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/36
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1(config)# interface fc1/40
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1#

7. Verify that the ISL ports on the replacement switch are up:
   show interface brief

8. Adjust the zoning on the replacement switch to match the MetroCluster configuration:
   a. Distribute the zoning information from the healthy fabric.

Example

In this example, FC_switch_B_1 has been replaced and the zoning information is retrieved from FC_switch_A_1:

FC_switch_A_1(config-zone)# zoneset distribute full vsan 10
FC_switch_A_1(config-zone)# zoneset distribute full vsan 20
FC_switch_A_1(config-zone)# end

b. On the replacement switch, verify that the zoning information was properly retrieved from the healthy switch:
   show zone

Example

FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/4 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/4 swn 20:00:54:7f:ee:b8:24:c0
zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/2 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swn 20:00:54:7f:ee:b8:24:c0
zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/2 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#

c. Find the WWNs of the switches.
Example

In this example, the two switch WWNs are as follows:

- FC_switch_A_1: 20:00:54:7f:ee:b8:24:c0
- FC_switch_B_1: 20:00:54:7f:ee:c6:80:78

Switch WWN is 20:00:54:7f:ee:c6:80:78

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0

Example

Remove zone members that do not belong to the switch WWNs of the two switches.

In this example, no member interface in the output shows that the following members are not associated with the switch WWN of either of the switches in the fabric and must be removed:

- zone name FC-VI_Zone_1_10 vsan 10
  - interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
- zone name STOR_Zone_1_20_25A vsan 20
  - interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
- zone name STOR_Zone_1_20_25B vsan 20
  - interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  - interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50

The following example shows the removal of these interfaces:
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# no member interface fc1/10 swnn
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# no member interface fc1/11 swnn
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# no member interface fc1/8 swnn
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# no member interface fc1/9 swnn
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# no member interface fc1/10 swnn
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# no member interface fc1/11 swnn
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# save running-config startup-config
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# zoneset distribute full 10
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# zoneset distribute full 20
20:00:54:7f:ee:e3:86:50
FC_switch_B_1(config-zone)# end
20:00:54:7f:ee:e3:86:50
FC_switch_B_1# copy running-config startup-config

e. Add the ports of the replacement switch to the zones.

Example

All the cabling on the replacement switch must be the same as on the impaired switch:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
FC_switch_B_1(config-zone)# member interface fc1/1 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# member interface fc1/2 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# member interface fc1/5 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# member interface fc1/8 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# member interface fc1/9 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# member interface fc1/10 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# member interface fc1/11 swnn
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# save running-config startup-config
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# zoneset distribute full 10
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# zoneset distribute full 20
20:00:54:7f:ee:c6:80:78
FC_switch_B_1(config-zone)# end
20:00:54:7f:ee:c6:80:78
FC_switch_B_1# copy running-config startup-config
```

f. Verify that the zoning is properly configured:

```
show zone
```

Example

The following example output shows the three zones:
g. Enable the connectivity to storage and the controllers.

**Example**

The following example shows the port usage:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/1
FC_switch_A_1(config)# no shut
FC_switch_A_1(config)# interface fc1/4
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/2-3
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/5-6
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/7-8
FC_switch_A_1(config)# shut
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

9. 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:

```
microcluster check run
```
e. Display the results of the MetroCluster check:

```
metrocluster check show
```

f. Run Config Advisor.

*NetApp Downloads: Config Advisor*

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

### Changing speed of ISL ports on a Cisco FC switch

You might need to change the speed of ISL ports on a switch to improve the quality of the ISL. ISLs traveling greater distances might need their speed lowered to improve quality.

#### Before you begin

You must complete all the steps on both switches to ensure ISL connectivity.

#### Steps

1. Disable the ISL ports of the ISLs that you want to change the speed of on both switches in the fabric:

   ```
   FC_switch_A_1# config t
   Enter configuration commands, one per line. End with CTRL-Z after you have entered all of the configuration commands.
   
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# shut
   FC_switch_A_1(config)# end
   ```

2. Change the speed of the ISL ports on both switches in the fabric:

   ```
   FC_switch_A_1# config t
   Enter configuration commands, one per line. End with CTRL-Z after you have entered all of the configuration commands.
   
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# switchport speed 16000
   ```

   **Note:** Speeds for ports are 16 = 16,000 Gbps, 8 = 8,000 Gbps, 4 = 4,000 Gbps.

   Ensure that these ISL ports for your switch are listed in the *Fabric-attached MetroCluster Installation and Configuration Guide*.

3. Enable all ISL ports (if not enabled) on both switches in the fabric:

   ```
   FC_switch_A_1# config t
   Enter configuration commands, one per line. End with CTRL-Z after you have entered all of the configuration commands.
   
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# no shut
   FC_switch_A_1(config)# end
   ```

4. Verify the ISLs are established between both switches:
show topology isl

<table>
<thead>
<tr>
<th>Local PC Domain</th>
<th>Local SwName</th>
<th>Local Port</th>
<th>Remote Port</th>
<th>Remote SwName</th>
<th>Remote Domain</th>
<th>VSAN</th>
<th>Cost</th>
<th>I/F PC</th>
<th>I/F Stat</th>
<th>I/F Stat</th>
<th>Speed</th>
<th>Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x11</td>
<td>cisco9</td>
<td>fc1/36</td>
<td>fc1/36</td>
<td>cisco9</td>
<td>0xbc</td>
<td>1</td>
<td>1</td>
<td>up</td>
<td>up</td>
<td>16g</td>
<td>64g</td>
</tr>
<tr>
<td>1</td>
<td>0x11</td>
<td>cisco9</td>
<td>fc1/40</td>
<td>fc1/40</td>
<td>cisco9</td>
<td>0xbc</td>
<td>1</td>
<td>1</td>
<td>up</td>
<td>up</td>
<td>16g</td>
<td>64g</td>
</tr>
<tr>
<td>1</td>
<td>0x11</td>
<td>cisco9</td>
<td>fc1/44</td>
<td>fc1/44</td>
<td>cisco9</td>
<td>0xbc</td>
<td>1</td>
<td>1</td>
<td>up</td>
<td>up</td>
<td>16g</td>
<td>64g</td>
</tr>
<tr>
<td>1</td>
<td>0x11</td>
<td>cisco9</td>
<td>fc1/48</td>
<td>fc1/48</td>
<td>cisco9</td>
<td>0xbc</td>
<td>1</td>
<td>1</td>
<td>up</td>
<td>up</td>
<td>16g</td>
<td>64g</td>
</tr>
</tbody>
</table>

5. Repeat the procedure for the second switch fabric.

Adding ISLs to a Cisco switch

You might need to add ISLs to a switch if you are adding or upgrading hardware such as additional or faster controllers or faster switches.

Before you begin
Steps that are completed on one switch must also be completed on the other to ensure ISL connectivity.

Steps

1. Disable the ISL ports of the ISLs to be added on both switches in the fabric:

   FC_switch_A_1#confi t

   Enter the configuration commands, one per line. End with CTRL-Z after all the configuration commands have been entered.

   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# shut
   FC_switch_A_1(config)# end

2. Insert SFPs into the ports you are adding as ISL ports, and cable them according to the Installation and Configuration Guide.

   Ensure that these ports are listed in the Installation and Configuration Guide for the switch you are adding them to.

3. Configure the ISL ports in accordance with the Installation and Configuration Guide.

4. Enable all ISL ports (if not enabled) on both switches in the fabric:

   FC_switch_A_1# confi t

   Enter the configuration commands, one per line. End with CTRL-Z.

   FC_switch_A_1# interface fc1/36
   FC_switch_A_1(config-if)# no shut
   FC_switch_A_1(config)# end

5. Verify the ISLs are established between both switches:

   show topology isl

6. Repeat the procedure on the second fabric:
<table>
<thead>
<tr>
<th></th>
<th>MetroCluster Service and Expansion Guide</th>
<th>1 0x11 cisco9 fcl/36 fcl/36 cisco9 0xbc</th>
<th>1 1 15 up up 16g 64g</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 0x11 cisco9 fcl/40 fcl/40 cisco9 0xbc</td>
<td>1 1 15 up up 16g 64g</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 0x11 cisco9 fcl/44 fcl/44 cisco9 0xbc</td>
<td>1 1 15 up up 16g 64g</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 0x11 cisco9 fcl/48 fcl/48 cisco9 0xbc</td>
<td>1 1 15 up up 16g 64g</td>
</tr>
</tbody>
</table>
Performing IP switch maintenance and replacement

If necessary, you can nondisruptively replace the IP switches or upgrade their firmware in the MetroCluster configuration.

Renaming a Cisco IP switch

You might need to rename a Cisco IP switch to provide consistent naming throughout your configuration.

About this task
In the examples in this task, the switch name is changed from myswitch to IP_switch_A_1.

Steps

1. Enter global configuration mode:

   `configure terminal`

   **Example**
   The following example shows the configuration mode prompt. Both prompts show the switch name of myswitch.

   ```
   myswitch# configure terminal
   myswitch(config)#
   ```

2. Rename the switch:

   `switchname new-switch-name`

   If you are renaming both switches in the fabric, use the same command on each switch.

   **Example**
   The CLI prompt changes to reflect the new name:

   ```
   myswitch(config)# switchname IP_switch_A_1
   IP_switch_A_1(config)#
   ```

3. Exit configuration mode:

   `exit`

   **Example**
   The top-level switch prompt is displayed:

   ```
   IP_switch_A_1(config)# exit
   IP_switch_A_1#
   ```

4. Copy the current running configuration to the startup configuration file:

   `copy running-config startup-config`
5. Verify that the switch name change is visible from the ONTAP cluster prompt.
   Note that the new switch name is shown, and the old switch name (myswitch) does not appear.

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

   b. Display the attached devices:
      
      network device-discovery show

   c. Return to admin privilege mode:
      
      set -privilege admin

**Example**

The following example shows that the switch appears with the new name, IP_switch_A_1:

```
cluster_A::storage show> set advanced
Warning: These advanced commands are potentially dangerous; use them only when directed
to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show

<table>
<thead>
<tr>
<th>Node/Protocol</th>
<th>Local Port</th>
<th>Device</th>
<th>Interface</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_2/cdp</td>
<td>e0M</td>
<td>LF01-410J53.mycompany.com(SAL18516DZY)</td>
<td>Ethernet125/1/28</td>
<td>N9K-C9372PX</td>
</tr>
<tr>
<td></td>
<td>e1a</td>
<td>IP_switch_A_1(FOC21211RBU)</td>
<td>Ethernet1/2</td>
<td>N3K-C3232C</td>
</tr>
<tr>
<td></td>
<td>e1b</td>
<td>IP_switch_A_1(FOC21211RBU)</td>
<td>Ethernet1/10</td>
<td>N3K-C3232C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node_A_1/cdp</td>
<td>e0M</td>
<td>LF01-410J53.mycompany.com(SAL18516DZY)</td>
<td>Ethernet125/1/26</td>
<td>N9K-C9372PX</td>
</tr>
<tr>
<td></td>
<td>e0a</td>
<td>IP_switch_A_2(FOC21211RB5)</td>
<td>Ethernet1/1</td>
<td>N3K-C3232C</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>IP_switch_A_2(FOC21211RB5)</td>
<td>Ethernet1/9</td>
<td>N3K-C3232C</td>
</tr>
<tr>
<td></td>
<td>e1a</td>
<td>IP_switch_A_1(FOC21211RBU)</td>
<td>Ethernet1/18</td>
<td>N9K-C9372PX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
16 entries were displayed.
```
Changing ISL port speed or adding ISL ports on a Cisco IP switch

You might need to change the speed of ISL ports on a switch to improve the quality of the ISL. ISLs traveling greater distances might require lower speeds to improve quality. You also might need to increase the speed of ISL ports to take advantage of system upgrades and add ISLs to a Cisco IP switch if you are adding or upgrading hardware.

About this task

You must complete all the steps on both switches to ensure ISL connectivity.

The following procedure assumes you are replacing a 10-Gb ISL connected at switch port Eth1/24/1 with two 100-Gb ISLs that are connected to switch ports 17 and 18.

Steps

1. Disable the ISL ports of the ISLs on both switches in the fabric that you want to change.

   You must enter only one configuration command for each line and press Ctrl-Z after you have entered all the commands, as shown in the following example:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/24/1
   switch_A_1(config-if)# shut
   switch_A_1(config-if)#
   switch_A_1#
   switch_B_1# conf t
   switch_B_1(config)# int eth1/24/1
   switch_B_1(config-if)# shut
   switch_B_1(config-if)#
   switch_B_1#
   ```

2. Disable the ISL ports that you are connecting to the new 100-Gb ISLs.

   In this example, you should disable ISL ports 17 and 18.

3. Remove the existing cables and transceivers.

4. Change the ISL port as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>To change the speed of an ISL port...</td>
<td>Cable the new ISLs to the designated ports according to their speeds. You must ensure that these ISL ports for your switch are listed in the MetroCluster IP Installation and Configuration Guide.</td>
</tr>
<tr>
<td>To add an ISL...</td>
<td>Insert QFSPs into the ports you are adding as ISL ports. Ensure they are listed in the MetroCluster IP Installation and Configuration Guide and cable them according to this guide.</td>
</tr>
</tbody>
</table>

5. Enable all ISL ports (if not enabled) on both switches in the fabric beginning with the following command:

   ```
   switch_A_1# conf t
   ```

   You must enter only one configuration command per line and press Ctrl-Z after you have entered all the commands:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/17
   switch_A_1(config-if)# no shut
   switch_A_1(config-if)# int eth1/18
   switch_A_1(config-if)# no shut
   ```
6. Verify that the ISLs are established between both switches:

```
switch_A_1# show int eth1/17,eth1/18 brief
```

You should see the ISL interfaces in the command output as shown in the following example:

<table>
<thead>
<tr>
<th>Ethernet Interface</th>
<th>VLAN</th>
<th>Type</th>
<th>Mode</th>
<th>Status</th>
<th>Reason</th>
<th>Speed</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/17</td>
<td>10</td>
<td>eth</td>
<td>access</td>
<td>up</td>
<td>none</td>
<td>100G(D)</td>
<td>10</td>
</tr>
<tr>
<td>Eth1/18</td>
<td>10</td>
<td>eth</td>
<td>access</td>
<td>up</td>
<td>none</td>
<td>100G(D)</td>
<td>10</td>
</tr>
</tbody>
</table>

```
switch_B_1# show int eth1/17,eth1/18 brief
```

<table>
<thead>
<tr>
<th>Ethernet Interface</th>
<th>VLAN</th>
<th>Type</th>
<th>Mode</th>
<th>Status</th>
<th>Reason</th>
<th>Speed</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/17</td>
<td>10</td>
<td>eth</td>
<td>access</td>
<td>up</td>
<td>none</td>
<td>100G(D)</td>
<td>10</td>
</tr>
<tr>
<td>Eth1/18</td>
<td>10</td>
<td>eth</td>
<td>access</td>
<td>up</td>
<td>none</td>
<td>100G(D)</td>
<td>10</td>
</tr>
</tbody>
</table>

Identifying storage in a MetroCluster IP configuration

If you need to replace a drive or shelf module, you first need to identify the location.

Identification of local and remote shelves

When you view shelf information from a MetroCluster site, all remote drives are on 0m, the virtual iSCSI host adapter. This means that the drives are accessed via the MetroCluster IP interfaces. All other drives are local.

After identifying whether a shelf is remote (on 0m), you can further identify the drive or shelf by the serial number or, depending on shelf ID assignments in your configuration, by shelf ID.

**Note:** In MetroCluster IP configurations running ONTAP 9.4, the shelf ID is not required to be unique between the MetroCluster sites. This includes both internal shelves (0) and external shelves. The serial number is consistent when viewed from any node on either MetroCluster site.

With the drive or shelf module identified, you can replace the component using the appropriate procedure.

DS460C, DS224C, and DS212C Disk Shelves: Service Guide

Example of sysconfig -a output

The following example uses the `sysconfig -a` command to show the devices on a node in the MetroCluster IP configuration. This node has the following shelves and devices attached:

- slot 0: Internal drives (local drives)
- slot 3: External shelf ID 75 and 76 (local drives)
- slot 0: Virtual iSCSI host adapter 0m (remote drives)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 111111111 (node_A_1); partner ID: 222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)

slot 0: NVMe Disks
  0 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3BBT2A0J500528)
  1 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3BBT2A0J500735)

slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
  MFG Part Number: Microsemi Corp. 110-03801 rev. A0
  Part number: 111-03801+A0
  Serial number: 7A1063AP14B
  Date Code: 20170320
  Firmware rev: 03.08.09.00
  Base WWN: 5:0000d1:702e69e:80
  Mini-SAS HD Vendor: Molex Inc.
  Mini-SAS HD Part Number: 112-00436+A0
  Mini-SAS HD Type: Passive Copper (unequalized) 0.5m ID:00
  Mini-SAS HD Serial Number: 614130640
```

95
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number: Microsemi Corp. 110-03801 rev. A0
Part number: 111-03801+A0
Serial number: 7A1063AF14B
Date Code: 20170320
Firmware rev: 03.08.09.00
Base WWN: 5:0000d1:702e69e:88
Phy State: [0] Enabled, 12.0 Gb/s
[1] Enabled, 12.0 Gb/s
[2] Enabled, 12.0 Gb/s
[3] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor: Molex Inc.
Mini-SAS HD Part Number: 112-00436+A0
Mini-SAS HD Type: Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691

75.0 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect (S20KNY5G01805)
75.1 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect (S20KNY5G02050)
75.2 : NETAPP X438_PMM2400MCTO NA04 381.3GB 520B/sect (25M0A03WT2KA)
75.3 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect (S20KNY5G01793)

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number: Microsemi Corp. 110-03801 rev. A0
Part number: 111-03801+A0
Serial number: 7A1063AF14B
Date Code: 20170320
Firmware rev: 03.08.09.00
Base WWN: 5:0000d1:702e69e:8c
Phy State: [4] Enabled, 12.0 Gb/s
[5] Enabled, 12.0 Gb/s
[6] Enabled, 12.0 Gb/s
[7] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor: Molex Inc.
Mini-SAS HD Part Number: 112-00436+A0
Mini-SAS HD Type: Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690

75.0 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect (S20KNY5G01805)
75.1 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect (S20KNY5G02050)
75.2 : NETAPP X438_PMM2400MCTO NA04 381.3GB 520B/sect (25M0A03WT2KA)

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+

slot 0: Virtual iSCSI Host Adapter 0m
  0.0 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500690)
  0.1 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500571)
  0.2 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500323)
  0.3 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500724)
  0.4 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500734)
  0.5 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500598)
  0.12 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J501094)
  0.13 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect (S3NBNX0J500519)

Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
Hot-adding storage to a MetroCluster FC configuration

You can add storage to a MetroCluster FC configuration without bringing down the system. The procedure you use depends on the type of MetroCluster FC configuration and whether you are adding a single disk shelf to an existing stack or an entire stack.

Choices

• Hot-adding a SAS disk shelf in a direct-attached MetroCluster FC configuration using SAS optical cables on page 97
• Hot-adding SAS storage to a bridge-attached MetroCluster FC configuration on page 97

Hot-adding a SAS disk shelf in a direct-attached MetroCluster FC configuration using SAS optical cables

You can use SAS optical cables to hot-add a SAS disk shelf to an existing stack of SAS disk shelves in a direct-attached MetroCluster FC configuration, or as a new stack to a SAS HBA or an onboard SAS port on the controller.

About this task

• This procedure is nondisruptive and takes approximately two hours to complete.
• You need the admin password and access to an FTP or SCP server.

This task applies to a MetroCluster FC configuration in which the storage is connected directly to the storage controllers with SAS cables. It does not apply to MetroCluster FC configurations using FC-to-SAS bridges or FC switch fabrics.

Step

1. Follow the instructions for hot-adding a SAS disk shelf in the Installation Guide for your disk shelf model to perform the following tasks to hot-add a disk shelf:
   a. Install a disk shelf for a hot-add.
   b. Turn on the power supplies and set the shelf ID for a hot-add.
   c. Cable the hot-added disk shelf.
   d. Verify SAS connectivity.

   *NetApp Documentation: Disk Shelves*

Hot-adding SAS storage to a bridge-attached MetroCluster FC configuration

You can hot-add either an individual SAS disk shelf or a stack and set of bridges to an existing MetroCluster system.

These procedures apply to MetroCluster FC configurations using FC-to-SAS bridges that are either directly attached to the storage controllers or attached to an FC fabric.
These procedures are nondisruptive and take approximately four hours to complete.
You need the admin password and access to an FTP or SCP server.

Choices
• Hot-adding a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges on page 98
• Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system on page 104
• Hot-adding a SAS disk shelf to a stack of SAS disk shelves on page 115

Hot-adding a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges
You can hot-add a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges that have available ports.

Before you begin
• You must have downloaded the latest disk and disk shelf firmware.
• All of the disk shelves in the MetroCluster configuration (both the new shelves and existing shelves) must be running the same firmware version.
  NetApp Downloads: Disk Drive and Firmware
  NetApp Downloads: Disk Shelf Firmware
• The FibreBridge 7500N bridges must be connected and have available SAS ports.

About this task
This procedure is written with the assumption that you are using the recommended bridge management interfaces: the ATTO ExpressNA V GUI and the ATTO QuickNA V utility.

You can use the ATTO ExpressNA V GUI to configure and manage a bridge, and to update the bridge firmware. You can use the ATTO QuickNA V utility to configure the bridge Ethernet management 1 port.

You can use other management interfaces, if required. These options include using a serial port or Telnet to configure and manage a bridge and to configure the Ethernet management 1 port, and using FTP to update the bridge firmware. If you choose any of these management interfaces, you must meet the applicable requirements in Other bridge management interfaces on page 58.

Attention: If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

Steps
1. Properly ground yourself.
2. From the console of either controller, verify that your system has disk autoassignment enabled:
   storage disk option show
   The Auto Assign column indicates whether disk autoassignment is enabled.

<table>
<thead>
<tr>
<th>Node</th>
<th>Bkg. FW. Upd</th>
<th>Auto Copy</th>
<th>Auto Assign</th>
<th>Auto Assign Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
<tr>
<td>node_A_2</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
</tbody>
</table>

2 entries were displayed.
3. Disable the switch ports for the new stack.

4. Update the FibreBridge firmware on each bridge.

5. On each bridge in the pair, enable the SAS port that will connect to the new stack:

   \texttt{SASPortEnable \textit{port-letter}}

   The same SAS port (B, C, or D) must be used on both bridges.

6. Save the configuration and reboot each bridge:

   \texttt{SaveConfiguration Restart}

7. Cable the disk shelves to the bridges:

   a. Daisy-chain the disk shelves in each stack.

   The \textit{Installation and Service Guide} for your disk shelf model provides detailed information about daisy-chaining disk shelves.

   \texttt{NetApp Documentation: Disk Shelves}

   b. For each stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and then cable IOM B of the last shelf to SAS port A on FibreBridge B

   Fabric-attached MetroCluster installation and configuration

   Stretch MetroCluster installation and configuration

   Each bridge has one path to its stack of disk shelves; bridge A connects to the A-side of the stack through the first shelf, and bridge B connects to the B-side of the stack through the last shelf.

   \textbf{Note:} The bridge SAS port B is disabled.

8. Verify that each bridge can detect all of the disk drives and disk shelves to which the bridge is connected.

<table>
<thead>
<tr>
<th>If you are using the...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTO ExpressNAV GUI</td>
<td>a. In a supported web browser, enter the IP address of a bridge in the browser box. You are brought to the ATTO FibreBridge home page, which has a link.</td>
</tr>
<tr>
<td></td>
<td>b. Click the link, and then enter your user name and the password that you designated when you configured the bridge. The ATTO FibreBridge status page appears with a menu to the left.</td>
</tr>
<tr>
<td></td>
<td>c. Click \textbf{Advanced} in the menu.</td>
</tr>
<tr>
<td></td>
<td>d. View the connected devices: \texttt{sastargets}</td>
</tr>
<tr>
<td></td>
<td>e. Click \texttt{Submit}.</td>
</tr>
</tbody>
</table>

Serial port connection

View the connected devices:

\texttt{sastargets} |

The output shows the devices (disks and disk shelves) to which the bridge is connected. The output lines are sequentially numbered so that you can quickly count the devices.

\textbf{Note:} If the text response truncated appears at the beginning of the output, you can use Telnet to connect to the bridge, and then view all of the output by using the \texttt{sastargets} command.
Example

The following output shows that 10 disks are connected:

<table>
<thead>
<tr>
<th>Tgt</th>
<th>VendorID</th>
<th>ProductID</th>
<th>Type</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CLE300009940UHVJ</td>
</tr>
<tr>
<td>1</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1ELF600009940V1BV</td>
</tr>
<tr>
<td>2</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G3W00009940U2M0</td>
</tr>
<tr>
<td>3</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1EWM00009940U1XS</td>
</tr>
<tr>
<td>4</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLE00009940G8YU</td>
</tr>
<tr>
<td>5</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLF00009940TZK2</td>
</tr>
<tr>
<td>6</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CEB400009939GMXL</td>
</tr>
<tr>
<td>7</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G7A900009939FNTT</td>
</tr>
<tr>
<td>8</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FY0T00009940G8PA</td>
</tr>
<tr>
<td>9</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FXW600009940VERQ</td>
</tr>
</tbody>
</table>

9. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

<table>
<thead>
<tr>
<th>If the output is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Repeat Step 8 on page 99 for each remaining bridge.</td>
</tr>
<tr>
<td>Not correct</td>
<td>a. Check for loose SAS cables or correct the SAS cabling by repeating Step 7 on page 99.</td>
</tr>
<tr>
<td></td>
<td>b. Repeat Step 8 on page 99.</td>
</tr>
</tbody>
</table>

10. Cable each bridge to the local FC switches, using the cabling shown in the table for your configuration, switch model, and FC-to-SAS bridge model:

*Note:* The Brocade and Cisco switches use different port numbering, as shown in the following tables

- On Brocade switches, the first port is numbered “0”.
- On Cisco switches, the first port is numbered “1”.

<table>
<thead>
<tr>
<th>Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DR GROUP 1</strong></td>
</tr>
<tr>
<td><strong>Component</strong></td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Stack 1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Stack 2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_3a</td>
<td>FC1 12</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
<td>- 12</td>
</tr>
<tr>
<td></td>
<td>bridge_x_3b</td>
<td>FC1 13</td>
<td>- 13</td>
<td>- 13</td>
<td>- 13</td>
<td>- 13</td>
<td>- 13</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_ya</td>
<td>FC1 14</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
<td>- 14</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-- 15</td>
<td>-- 15</td>
<td>-- 15</td>
<td>-- 15</td>
<td>-- 15</td>
<td>-- 15</td>
</tr>
</tbody>
</table>

Note: Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620 and G630 switches.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_51a</td>
<td>FC1 26</td>
<td>- 32</td>
<td>- 32</td>
<td>- 56</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 26</td>
<td>- 32</td>
<td>- 32</td>
<td>- 56</td>
</tr>
<tr>
<td></td>
<td>bridge_x_51b</td>
<td>FC1 27</td>
<td>- 33</td>
<td>- 33</td>
<td>- 57</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 27</td>
<td>- 33</td>
<td>- 33</td>
<td>- 57</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52a</td>
<td>FC1 30</td>
<td>- 34</td>
<td>- 34</td>
<td>- 58</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 30</td>
<td>- 34</td>
<td>- 34</td>
<td>- 58</td>
</tr>
<tr>
<td></td>
<td>bridge_x_52b</td>
<td>FC1 31</td>
<td>- 35</td>
<td>- 35</td>
<td>- 59</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 31</td>
<td>- 35</td>
<td>- 35</td>
<td>- 59</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53a</td>
<td>FC1 32</td>
<td>- 36</td>
<td>- 36</td>
<td>- 60</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 32</td>
<td>- 36</td>
<td>- 36</td>
<td>- 60</td>
</tr>
<tr>
<td></td>
<td>bridge_x_53b</td>
<td>FC1 33</td>
<td>- 37</td>
<td>- 37</td>
<td>- 61</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>- 33</td>
<td>- 37</td>
<td>- 37</td>
<td>- 61</td>
</tr>
</tbody>
</table>
### Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack y</td>
<td>bridge_x_5ya</td>
<td>FC1</td>
<td>34</td>
<td>-</td>
<td>38</td>
<td>-</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>34</td>
<td>-</td>
<td>38</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_5yb</td>
<td>FC1</td>
<td>35</td>
<td>-</td>
<td>39</td>
<td>-</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>35</td>
<td>-</td>
<td>39</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 36 - 39 in G620 and G630 switches.

### Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>8</td>
<td>-</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
<td>11</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>11</td>
<td>-</td>
<td>11</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 12 - 17, 20 and 21 in G620 and G630 switches.
Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

<table>
<thead>
<tr>
<th>DR GROUP 2</th>
<th>Brocade G620, Brocade G630</th>
<th>Brocade 6510, Brocade DCX 8510-8</th>
<th>Brocade 6520</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_51a 26</td>
<td>32</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>bridge_x_51b -</td>
<td>26</td>
<td>-</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52a 27</td>
<td>33</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>bridge_x_52b -</td>
<td>27</td>
<td>-</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53a 30</td>
<td>34</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>bridge_x_54b -</td>
<td>30</td>
<td>-</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_ya 31</td>
<td>35</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>bridge_x_yb -</td>
<td>31</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 32 - 39 in G620 and G630 switches.

11. Update the disk drive firmware to the most current version from the system console:
   ```
   disk_fw_update
   ```
   You must run this command on both controllers.

   *NetApp Downloads: Disk Drive and Firmware*

12. Update the disk shelf firmware to the most current version by using the instructions for the downloaded firmware.
   You can run the commands in the procedure from the system console of either controller.

   *NetApp Downloads: Disk Shelf Firmware*

13. If your system does not have disk autoassignment enabled, assign disk drive ownership.
   **Disk and aggregate management**
   
   **Note:** If you are splitting the ownership of a single stack of disk shelves among multiple controllers, you must disable disk autoassignment (storage disk option modify - autoassign off * from both nodes in the cluster) before assigning disk ownership; otherwise, when you assign any single disk drive, the remaining disk drives might be automatically assigned to the same controller and pool.
   
   **Note:** You must not add disk drives to aggregates or volumes until after the disk drive firmware and disk shelf firmware have been updated and the verification steps in this task have been completed.

14. Enable the switch ports for the new stack.

15. 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:
   
   \texttt{metrocluster\ show}

   d. Perform a MetroCluster check:
   
   \texttt{metrocluster\ check\ run}

   e. Display the results of the MetroCluster check:
   
   \texttt{metrocluster\ check\ show}

   f. Run Config Advisor.
   
   \textit{NetApp Downloads: Config Advisor}

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

16. If applicable, repeat this procedure for the partner site.

\textbf{Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system}

You can hot-add (nondisruptively add) an entire stack, including the bridges, to the MetroCluster system. There must be available ports on the FC switches and you must update switch zoning to reflect the changes.

\textbf{About this task}

- This procedure can be used to add a stack using either FibreBridge 7500N or 6500N bridges.
- This procedure is written with the assumption that you are using the recommended bridge management interfaces: the ATTO ExpressNA V GUI and the ATTO QuickNA V utility.
  - You use the ATTO ExpressNA V GUI to configure and manage a bridge, and to update the bridge firmware. You use the ATTO QuickNA V utility to configure the bridge Ethernet management 1 port.
  - You can use other management interfaces, if needed. These options include using a serial port or Telnet to configure and manage a bridge, and to configure the Ethernet management 1 port, and using FTP to update the bridge firmware. If you choose any of these management interfaces, your system must meet the applicable requirements in Other bridge management interfaces on page 58

\textbf{Steps}

1. Preparing to hot-add a stack of SAS disk shelves and bridges on page 104
2. Hot-adding a stack of SAS disk shelves and bridges on page 106

\textbf{Preparing to hot-add a stack of SAS disk shelves and bridges}

Preparing to hot-add a stack of SAS disk shelves and a pair of bridges involves downloading documents as well as the disk drive and disk shelf firmware.

\textbf{Before you begin}

- Your system must be a supported configuration and must be running a supported version of ONTAP.
  
  \textit{NetApp Interoperability Matrix Tool}

- All disk drives and disk shelves in the system must be running the latest firmware version.
You might want to update the disk and shelf firmware throughout the MetroCluster configuration prior to adding shelves.

**Upgrade, revert, or downgrade**

- Each FC switch must have one FC port available for one bridge to connect to it.
  
  **Note:** You might need to upgrade the FC switch depending on the FC switch compatibility.

- The computer you are using to set up the bridges must be running an ATTO supported web browser to use the ATTO ExpressNAV GUI: Internet Explorer 8 or 9, or Mozilla Firefox 3. The *ATTO Product Release Notes* have an up-to-date list of supported web browsers. You can access this document using the information in the steps.

**Steps**

1. Download or view the following documents from the NetApp Support Site:
   - *NetApp Interoperability Matrix Tool*
   - The *Installation and Service Guide* for your disk shelf model.
   - *NetApp Documentation: Disk Shelves*

2. Download content from the ATTO website and from the NetApp website:
   a. Go to the ATTO FibreBridge *Description* page.
      
      *NetApp Downloads: ATTO FibreBridge 7600N*
      *NetApp Downloads: ATTO FibreBridge 7500N*
      *NetApp Downloads: ATTO FibreBridge 6500N*
   b. Using the link on the ATTO FibreBridge *Description* page, access the ATTO web site and download the following:
      - *ATTO FibreBridge Installation and Operation Manual* for your bridge model.
      - ATTO QuickNAV utility (to the computer you are using for setup).
   c. Go to the ATTO FibreBridge Firmware *Download* page by clicking *Continue* at the end of the ATTO FibreBridge *Description* page, and then do the following:
      - Download the bridge firmware file as directed on the download page.
        In this step, you are only completing the download portion of the instructions provided in the links. You update the firmware on each bridge later, when instructed to do so in the *Hot-adding the stack of shelves* on page 106 section.
      - Make a copy of the ATTO FibreBridge Firmware Download page and release notes for reference later.

3. Download the latest disk and disk shelf firmware, and make a copy of the installation portion of the instructions for reference later.
   All disk shelves in the MetroCluster configuration (both the new shelves and existing shelves) must be running the same firmware version.
   
   **Note:** In this step, you are only completing the download portion of the instructions provided in the links and making a copy of the installation instructions. You update the firmware on each disk and disk shelf later, when instructed to do so in the *Hot-adding the stack of shelves* on page 106 section.
   a. Download the disk firmware and make a copy of the disk firmware instructions for reference later.
b. Download the disk shelf firmware and make a copy of the disk shelf firmware instructions for reference later.

*NetApp Downloads: Disk Shelf Firmware*

4. Gather the hardware and information needed to use the recommended bridge management interfaces—the ATTO ExpressNAV GUI and ATTO QuickNAV utility:
   a. Acquire a standard Ethernet cable to connect from the bridge Ethernet management 1 port to your network.
   b. Determine a non-default user name and password for accessing the bridges.
      It is recommended that you change the default user name and password.
   c. Obtain an IP address, subnet mask, and gateway information for the Ethernet management 1 port on each bridge.
   d. Disable VPN clients on the computer you are using for setup.
      Active VPN clients cause the QuickNAV scan for bridges to fail.

5. Acquire four screws for each bridge to flush-mount the bridge “L” brackets securely to the front of the rack.
   The openings in the bridge “L” brackets are compliant with rack standard ETA-310-X for 19-inch (482.6 mm) racks.

6. If necessary, update the FC switch zoning to accommodate the new bridges that are being added to the configuration.
   If you are using the Reference Configuration Files provided by NetApp, the zones have been created for all ports, so you do not need to make any zoning updates. There must be a storage zone for each switch port that connects to the FC ports of the bridge.

**Hot-adding a stack of SAS disk shelves and bridges**

You can hot-add a stack of SAS disk shelves and bridges to increase the capacity of the bridges.

**Before you begin**

The system must meet all of the requirements to hot-add a stack of SAS disk shelves and bridges.

*Preparing to hot-add a stack of SAS disk shelves and bridges* on page 104

**About this task**

- Hot-adding a stack of SAS disk shelves and bridges is a nondisruptive procedure if all of the interoperability requirements are met.
  *NetApp Interoperability Matrix Tool*
  Using the Interoperability Matrix Tool to find MetroCluster information on page 239
- Multipath HA is the only supported configuration for MetroCluster systems that are using bridges.
  Both controller modules must have access through the bridges to the disk shelves in each stack.
- You should hot-add an equal number of disk shelves at each site.
- If you will be using in-band management of the bridge rather than IP management, the steps for configuring the Ethernet port and IP settings can be skipped, as noted in the relevant steps.

**Attention:** If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.
Steps

1. Properly ground yourself.

2. From the console of either controller module, check whether your system has disk autoassignment enabled:

   `storage disk option show`

   The `Auto Assign` column indicates whether disk autoassignment is enabled.

<table>
<thead>
<tr>
<th>Node</th>
<th>BKg. FW. Upd.</th>
<th>Auto Copy</th>
<th>Auto Assign</th>
<th>Auto Assign Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
<tr>
<td>node_A_2</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
</tbody>
</table>

   2 entries were displayed.

3. Disable the switch ports for the new stack.

4. If configuring for in-band management, connect a cable from FibreBridge RS-232 serial port to the serial (COM) port on a personal computer.

   The serial connection will be used for initial configuration, and then in-band management via ONTAP and the FC ports can be used to monitor and manage the bridge.

5. If configuring for IP management, configure the Ethernet management 1 port for each bridge by following the procedure in section 2.0 of the *ATTO FibreBridge Installation and Operation Manual* for your bridge model.

   In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.

   When running QuickNAV to configure an Ethernet management port, only the Ethernet management port that is connected by the Ethernet cable is configured. For example, if you also wanted to configure the Ethernet management 2 port, you would need to connect the Ethernet cable to port 2 and run QuickNAV.

6. Configure the bridge.

   Be sure to make note of the user name and password that you designate.

   The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

   **Note:** Do not configure time synchronization on ATTO FibreBridge 7600N or 7500N. The time synchronization for ATTO FibreBridge 7600N or 7500N is set to the cluster time after the bridge is discovered by ONTAP. It is also synchronized periodically once a day. The time zone used is GMT and is not changeable.

   a. If configuring for IP management, configure the IP settings of the bridge.

      To set the IP address without the QuickNAV utility, you need to have a serial connection to the FibreBridge.

      **Example**

      If using the CLI, you must run the following commands:

      ```
      set ipaddress mpl ip-address
      set ipsubnetmask mpl subnet-mask
      set ipgateway mpl x.x.x.x
      set ipdhcp mpl disabled
      ```
set ethernetspeed mp1 1000

b. Configure the bridge name.

The bridges should each have a unique name within the MetroCluster configuration.

Example bridge names for one stack group on each site:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

Example

If using the CLI, you must run the following command:

set bridgename bridgename

c. If running ONTAP 9.4 or earlier, enable SNMP on the bridge:

set SNMP enabled

If running ONTAP 9.5 or later, ONTAP will use in-band monitoring via the FC connection to the bridge, so you should leave SNMP disabled.

7. Configure the bridge FC ports.

a. Configure the data rate/speed of the bridge FC ports.

The supported FC data rate depends on your model bridge.

- The FibreBridge 7600 bridge supports up to 32, 16, or 8 Gbps.
- The FibreBridge 7500 bridge supports up to 16, 8, or 4 Gbps.
- The FibreBridge 6500 bridge supports up to 8, 4, or 2 Gbps.

Note: The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

Example

If using the CLI, you must run the following command:

set FCDataRate port-number port-speed

b. If you are configuring a FibreBridge 7500N or 6500N bridge, configure the connection mode that the port uses to ptp.

Note: The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

Example

If using the CLI, you must run the following command:

set FCConnMode port-number ptp

c. If you are configuring a FibreBridge 7600N or 7500N bridge, you must configure or disable the FC2 port.

- If you are using the second port, you must repeat the previous substeps for the FC2 port.
• If you are not using the second port, then you must disable the port:

   **FCPortDisable port-number**

d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports:

   **SASPortDisable sas-port**

   **Note:** SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used. If only SAS port A is used, then SAS ports B, C, and D must be disabled.

8. Save the bridge's configuration and secure the bridge.

   a. Save the bridge's configuration.

      **Example**
      
      You must run the following commands:
      **SaveConfiguration**
      **FirmwareRestart**
      
      You are prompted to restart the bridge.

   b. If running ONTAP 9.5 or later, secure access to the bridge.
      
      Starting with ONTAP 9.5, you can secure access to the bridge to allow access only using in-band management through the FC ports.

      **Example**
      
      You must run the following command:
      **SecureBridge**

9. Update the FibreBridge firmware on each bridge.

10. Cable the disk shelves to the bridges:

    a. Daisy-chain the disk shelves in each stack.

       The **Installation Guide** for your disk shelf model provides detailed information about daisy-chaining disk shelves.

       **NetApp Documentation: Disk Shelves**

    b. For each stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and then cable IOM B of the last shelf to SAS port A on FibreBridge B.

       **Fabric-attached MetroCluster installation and configuration**

       **Stretch MetroCluster installation and configuration**

       Each bridge has one path to its stack of disk shelves; bridge A connects to the A-side of the stack through the first shelf, and bridge B connects to the B-side of the stack through the last shelf.

       **Note:** The bridge SAS port B is disabled.

11. Verify that each bridge can detect all of the disk drives and disk shelves to which the bridge is connected.
If you are using the...

<table>
<thead>
<tr>
<th>ATTO ExpressNAV GUI</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. In a supported web browser, enter the IP address of a bridge in the browser box. You are brought to the ATTO FibreBridge home page, which has a link.</td>
<td></td>
</tr>
<tr>
<td>b. Click the link, and then enter your user name and the password that you designated when you configured the bridge. The ATTO FibreBridge status page appears with a menu to the left.</td>
<td></td>
</tr>
<tr>
<td>c. Click Advanced in the menu.</td>
<td></td>
</tr>
<tr>
<td>d. View the connected devices: <code>sastargets</code></td>
<td></td>
</tr>
<tr>
<td>e. Click Submit.</td>
<td></td>
</tr>
</tbody>
</table>

The output shows the devices (disks and disk shelves) to which the bridge is connected. The output lines are sequentially numbered so that you can quickly count the devices.

**Note:** If the text `response truncated` appears at the beginning of the output, you can use Telnet to connect to the bridge, and then view all of the output by using the `sastargets` command.

**Example**

The following output shows that 10 disks are connected:

<table>
<thead>
<tr>
<th>Tgt</th>
<th>VendorID</th>
<th>ProductID</th>
<th>Type</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CLE300009940UHJV</td>
</tr>
<tr>
<td>1</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1ELF600009940V1BV</td>
</tr>
<tr>
<td>2</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G3E0000994002M0</td>
</tr>
<tr>
<td>3</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1EWM00009940U1X5</td>
</tr>
<tr>
<td>4</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLE00009940G8YU</td>
</tr>
<tr>
<td>5</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLF000099402ZK2</td>
</tr>
<tr>
<td>6</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1C38400009939MGXL</td>
</tr>
<tr>
<td>7</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G7A900009939FNTR</td>
</tr>
<tr>
<td>8</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FY0T00009940G8PA</td>
</tr>
<tr>
<td>9</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FX0W600009940VERQ</td>
</tr>
</tbody>
</table>

12. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

<table>
<thead>
<tr>
<th>If the output is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Repeat Step 11 on page 109 for each remaining bridge.</td>
</tr>
<tr>
<td>Not correct</td>
<td>a. Check for loose SAS cables or correct the SAS cabling by repeating Step 10 on page 109.</td>
</tr>
<tr>
<td></td>
<td>b. Repeat Step 11 on page 109.</td>
</tr>
</tbody>
</table>

13. If you are configuring a fabric-attached MetroCluster configuration, cable each bridge to the local FC switches, using the cabling shown in the table for your configuration, switch model, and FC-to-SAS bridge model:

**Note:** Brocade and Cisco switches use different port numbering, as shown in the following tables.
- On Brocade switches, the first port is numbered “0”.
- On Cisco switches, the first port is numbered “1”.

### Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade 6505</th>
<th>Brocade 6510, Brocade DCX 8510-8</th>
<th>Brocade 6520</th>
<th>Brocade G620, Brocade G630</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>8</td>
<td>-</td>
<td>8</td>
</tr>
<tr>
<td>bridge_x_1B</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>Stack 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_2B</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>11</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>Stack 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>12</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_3B</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>13</td>
<td>-</td>
<td>13</td>
</tr>
<tr>
<td>Stack y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_ya</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>14</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_yb</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>--</td>
<td>15</td>
<td>--</td>
<td>15</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620 and G630 switches.
### Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

#### DR GROUP 2

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_51a</td>
<td>FC1</td>
<td>26</td>
<td>-</td>
<td>32</td>
<td>-</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>26</td>
<td>-</td>
<td>32</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_51b</td>
<td>FC1</td>
<td>27</td>
<td>-</td>
<td>33</td>
<td>-</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>27</td>
<td>-</td>
<td>33</td>
<td>-</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52a</td>
<td>FC1</td>
<td>30</td>
<td>-</td>
<td>34</td>
<td>-</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>30</td>
<td>-</td>
<td>34</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_52b</td>
<td>FC1</td>
<td>31</td>
<td>-</td>
<td>35</td>
<td>-</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>31</td>
<td>-</td>
<td>35</td>
<td>-</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53a</td>
<td>FC1</td>
<td>32</td>
<td>-</td>
<td>36</td>
<td>-</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>32</td>
<td>-</td>
<td>36</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_53b</td>
<td>FC1</td>
<td>33</td>
<td>-</td>
<td>37</td>
<td>-</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>33</td>
<td>-</td>
<td>37</td>
<td>-</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_5ya</td>
<td>FC1</td>
<td>34</td>
<td>-</td>
<td>38</td>
<td>-</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>34</td>
<td>-</td>
<td>38</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_5yb</td>
<td>FC1</td>
<td>35</td>
<td>-</td>
<td>39</td>
<td>-</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>-</td>
<td>35</td>
<td>-</td>
<td>39</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 36 - 39 in G620 and G630 switches.

### Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

#### DR GROUP 1

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_1a</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1b</td>
<td>-</td>
<td>8</td>
<td>-</td>
<td>8</td>
<td>8</td>
<td>-</td>
</tr>
</tbody>
</table>
### Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

#### DR GROUP 1

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 2</td>
<td>bridge_x_2a</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_2b</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_3a</td>
<td>10</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_4b</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_ya</td>
<td>11</td>
<td>-</td>
<td>11</td>
<td>-</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bridge_x_yb</td>
<td>-</td>
<td>11</td>
<td>-</td>
<td>11</td>
<td>-</td>
<td>11</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 12 - 17, 20 and 21 in G620 and G630 switches.

### Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

#### DR GROUP 2

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade G620, Brocade G630</th>
<th>Brocade 6510, Brocade DCX 8510-8</th>
<th>Brocade 6520</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack 1</td>
<td>bridge_x_51a</td>
<td>26</td>
<td>-</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>bridge_x_51b</td>
<td>-</td>
<td>26</td>
<td>-</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52a</td>
<td>27</td>
<td>-</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>bridge_x_52b</td>
<td>-</td>
<td>27</td>
<td>-</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53a</td>
<td>30</td>
<td>-</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>bridge_x_54b</td>
<td>-</td>
<td>30</td>
<td>-</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_ya</td>
<td>31</td>
<td>-</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>bridge_x_yb</td>
<td>-</td>
<td>31</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 32 - 39 in G620 and G630 switches.

14. If you are configuring a bridge-attached MetroCluster system, cable each bridge to the controller modules:
a. Cable FC port 1 of the bridge to a 16 Gb or 8 Gb FC port on the controller module in cluster_A.

b. Cable FC port 2 of the bridge to the same speed FC port of the controller module in cluster_A.

c. Repeat these substeps on other subsequent bridges until all of the bridges have been cabled.

15. Update the disk drive firmware to the most current version from the system console:

   disk_fw_update

   You must run this command on both controller modules.

   NetApp Downloads: Disk Drive and Firmware

16. Update the disk shelf firmware to the most current version by using the instructions for the downloaded firmware.

   You can run the commands in the procedure from the system console of either controller module.

   NetApp Downloads: Disk Shelf Firmware

17. If your system does not have disk autoassignment enabled, assign disk drive ownership.

   Disk and aggregate management

   Note: If you are splitting the ownership of a single stack of disk shelves among multiple controller modules, you must disable disk autoassignment on both nodes in the cluster (storage disk option modify -autoassign off * ) before assigning disk ownership; otherwise, when you assign any single disk drive, the remaining disk drives might be automatically assigned to the same controller module and pool.

   Note: You must not add disk drives to aggregates or volumes until after the disk drive firmware and disk shelf firmware have been updated and the verification steps in this task have been completed.

18. Enable the switch ports for the new stack.

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

   a. Check whether the system is multipathed:

      node run -node (node name) sysconfig -a

   b. Check for any health alerts on both clusters:

      system health alert show

   c. Confirm the MetroCluster configuration and that the operational mode is normal:

      metrocluster show

   d. Perform a MetroCluster check:

      metrocluster check run

   e. Display the results of the MetroCluster check:

      metrocluster check show

   f. Run Config Advisor.

      NetApp Downloads: Config Advisor

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

20. If applicable, repeat this procedure for the partner site.
Related concepts

In-band management of the FC-to-SAS bridges on page 59

Hot-adding a SAS disk shelf to a stack of SAS disk shelves

You can hot-add one or more SAS disk shelves to a stack of SAS disk shelves.

Steps

1. Preparing to hot-add SAS disk shelves on page 115
2. Hot-adding a disk shelf on page 116

Preparing to hot-add SAS disk shelves

Preparing to hot-add a SAS disk shelf involves downloading documents as well as the disk drive and disk shelf firmware.

Before you begin

• Your system must be a supported configuration and must be running a supported version of ONTAP.
• All disk drives and disk shelves in the system must be running the latest firmware version. You might want to update the disk and shelf firmware throughout the MetroCluster configuration prior to adding shelves.

Upgrade, revert, or downgrade

Note: A mix of IOM12 (SAS-3) modules and IOM3/IOM6 modules is not supported within the same stack. If you cannot upgrade or downgrade the IOM modules on the existing stack or the new shelf that is to be added to a supported combination of IOM modules, you need to do one of the following:
• Start a new stack on a new SAS port (if supported by the bridge-pair).
• Start a new stack on an additional bridge-pair.

Steps

1. Download or view the following documents from the NetApp Support Site:
   • NetApp Interoperability Matrix Tool
   • The Installation Guide for your disk shelf model.

NetApp Documentation: Disk Shelves

2. Verify that the disk shelf you are hot-adding is supported.

NetApp Interoperability Matrix Tool

3. Download the latest disk and disk shelf firmware:
   
   Note: In this step, you are only completing the download portion of the instructions provided in the links. You need to follow the steps found in the Hot-adding a disk shelf on page 116 section for installing the disk shelf.

   a. Download the disk firmware and make a copy of the disk firmware instructions for reference later.

NetApp Downloads: Disk Drive and Firmware
Hot-add a disk shelf
You can hot-add a disk shelf when you want to increase storage without any reduction in performance.

Before you begin
- The system must meet all of the requirements in Preparing to hot-add SAS disk shelves on page 115.
- Your environment must meet one of the following scenarios to hot-add a shelf:
  - You have two FibreBridge 7500N bridges connected to a stack of SAS disk shelves.
  - You have one FibreBridge 7500N bridge and one FibreBridge 6500N bridge connected to a stack of SAS disk shelves.
  - You have two FibreBridge 6500N bridges connected to a stack of SAS disk shelves.

About this task
- This procedure is for hot-adding a disk shelf to the last disk shelf in a stack.
  This procedure is written with the assumption that the last disk shelf in a stack is connected from IOM A to bridge A and from IOM B to bridge B.
- This is a nondisruptive procedure.
- You should hot-add an equal number of disk shelves at each site.
- If you are hot-adding more than one disk shelf, you must hot-add one disk shelf at a time.
  Note: Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks.

Attention: Hot-adding a disk shelf requires you to update the disk drive firmware on the hot-added disk shelf by running the storage disk firmware update command in advanced mode. Running this command can be disruptive if the firmware on existing disk drives in your system is an older version.

Attention: If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

Steps
1. Properly ground yourself.
2. Verify disk shelf connectivity from the system console of either controller:
   `sysconfig -v`
   The output is similar to the following:
   - Each bridge on a separate line and under each FC port to which it is visible; for example, hot-adding a disk shelf to a set of FibreBridge 7500N bridges results in the following output:
     ```
     FC-to-SAS Bridge:
cisco_A_1-1:9.126L0: ATTO FibreBridge7500N 2.10 FB7500N100189
cisco_A_1-2:1.126L0: ATTO FibreBridge7500N 2.10 FB7500N100162
     ```
Hot-adding storage to a MetroCluster FC configuration | 117

- Each disk shelf on a separate line under each FC port to which it is visible:

<table>
<thead>
<tr>
<th>Shelf</th>
<th>0: IOM6 Firmware rev. IOM6 A: 0173 IOM6 B: 0173</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shelf</td>
<td>1: IOM6 Firmware rev. IOM6 A: 0173 IOM6 B: 0173</td>
</tr>
</tbody>
</table>

- Each disk drive on a separate line under each FC port to which it is visible:

<table>
<thead>
<tr>
<th>Disk Drive</th>
<th>Model</th>
<th>Capacity</th>
<th>LUN</th>
<th>Size (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco_A_1-1:9.126L1</td>
<td>NETAPP X421_HC0BD450A10 NA01</td>
<td>418.0GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cisco_A_1-1:9.126L2</td>
<td>NETAPP X421_HC0BD450A10 NA01</td>
<td>418.0GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Check whether your system has disk autoassignment enabled from the console of either controller:

```bash
storage disk option show
```

The autoassignment policy is shown in the Auto Assign column.

<table>
<thead>
<tr>
<th>Node</th>
<th>BKg. FW. Upd.</th>
<th>Auto Copy</th>
<th>Auto Assign</th>
<th>Auto Assign Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
<tr>
<td>node_A_2</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
</tbody>
</table>

2 entries were displayed.

4. If your system does not have disk autoassignment enabled, or if disk drives in the same stack are owned by both controllers, assign disk drives to the appropriate pools.

**Disk and aggregate management**

**Note:** If you are splitting a single stack of disk shelves between two controllers, disk autoassignment must be disabled before you assign disk ownership; otherwise, when you assign any single disk drive, the remaining disk drives might be automatically assigned to the same controller and pool.

The `storage disk option modify -node node-name -autoassign off` command disables disk autoassignment.

**Note:** Disk drives must not be added to aggregates or volumes until the disk drive and disk shelf firmware have been updated.

5. Update the disk shelf firmware to the most current version by using the instructions for the downloaded firmware.

You can run the commands in the procedure from the system console of either controller.

**NetApp Downloads: Disk Shelf Firmware**

6. Install and cable the disk shelf:

Note the following considerations:

- For FibreBridge 6500N bridges:
  - Wait at least 10 seconds before connecting the port. The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place and the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

- For FibreBridge 7500N bridges:
  - Do not force a connector into a port. The mini-SAS cables are keyed; when oriented correctly into a SAS port, the SAS cable clicks into place and the disk shelf SAS port LNK LED
illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented up (on the topside of the connector).

a. Install the disk shelf, power it on, and set the shelf ID.

The *Installation Guide* for your disk shelf model provides detailed information about installing disk shelves.

*NetApp Documentation: Disk Shelves*

**Note:** You must power-cycle the disk shelf and keep the shelf IDs unique for each SAS disk shelf within the entire storage system.

b. Disconnect the SAS cable from the IOM B port of the last shelf in the stack, and then reconnect it to the same port in the new shelf.

The other end of this cable remains connected to bridge B.

c. Daisy-chain the new disk shelf by cabling the new shelf IOM ports (of IOM A and IOM B) to the last shelf IOM ports (of IOM A and IOM B).

The *Installation Guide* for your disk shelf model provides detailed information about daisy-chaining disk shelves.

*NetApp Documentation: Disk Shelves*

7. Update the disk drive firmware to the most current version from the system console.

*NetApp Downloads: Disk Drive and Firmware*

a. Change to the advanced privilege level:

```
set -privilege advanced
```

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

b. Update the disk drive firmware to the most current version from the system console:

```
storage disk firmware update
```

c. Return to the admin privilege level:

```
set -privilege admin
```

d. Repeat the previous substeps on the other controller.

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

a. Check whether the system is multipathed:

```
node run -node (node name) sysconfig -a
```

b. Check for any health alerts on both clusters:

```
system health alert show
```

c. Confirm the MetroCluster configuration and that the operational mode is normal:

```
metrocluster show
```

d. Perform a MetroCluster check:

```
metrocluster check run
```

e. Display the results of the MetroCluster check:

```
metrocluster check show
```

f. Run Config Advisor.
NetApp Downloads: Config Advisor

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

9. If you are hot-adding more than one disk shelf, repeat the steps, starting with step 2 on page 116, for each disk shelf that you are hot-adding.
Hot-removing storage from a MetroCluster FC configuration

You can hot-remove drive shelves—physically remove shelves that have had the aggregates removed from the drives—from a MetroCluster FC configuration that is up and serving data. You can hot-remove one or more shelves from anywhere within a stack of shelves or remove a stack of shelves.

Before you begin

- Your system must be a multipath HA, multipath, quad-path HA, or quad-path configuration.
- In a four-node MetroCluster FC configuration, the local HA pair cannot be in a takeover state.
- You must have already removed all aggregates from the drives in the shelves that you are removing.

Attention: If you attempt this procedure on non-MetroCluster FC configurations with aggregates on the shelf you are removing, you could cause the system to fail with a multidrive panic. Removing aggregates involves splitting the mirrored aggregates on the shelves you are removing, and then re-creating the mirrored aggregates with another set of drives.

Disk and aggregate management

- You must have removed drive ownership after removing the aggregates from the drives in the shelves that you are removing.

Disk and aggregate management

- If you are removing one or more shelves from within a stack, you must have factored the distance to bypass the shelves that you are removing.
  If the current cables are not long enough, you need to have longer cables available.

About this task

This task applies to the following MetroCluster FC configurations:

- Direct-attached MetroCluster FC configurations, in which the storage shelves are directly connected to the storage controllers with SAS cables
- Fabric-attached or bridge-attached MetroCluster FC configurations, in which the storage shelves are connected using FC-to-SAS bridges

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:
      ```
      node run -node (node name) sysconfig -a
      ```
   b. Check for any health alerts on both clusters:
      ```
      system health alert show
      ```
   c. Confirm the MetroCluster configuration and that the operational mode is normal:
      ```
      metrocluster show
      ```
   d. Perform a MetroCluster check:
      ```
      metrocluster check run
      ```
e. Display the results of the MetroCluster check:
   
   `metrocluster check show`

f. Run Config Advisor.
   
   *NetApp Downloads: Config Advisor*

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

2. Set the privilege level to advanced:
   
   `set -privilege advanced`

3. Verify that no mailbox drive is on the shelves:
   
   `storage failover mailbox-disk show`

4. Remove the shelf according to the steps for the relevant scenario.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Steps</th>
</tr>
</thead>
</table>
| To remove an aggregate when the shelf contains either unmirrored, mirrored, or both types of aggregate... | a. Use the `storage aggregate delete -aggregate aggregate name` command to remove the aggregate.  

b. Use the standard procedure to remove ownership of all drives in that shelf, and then physically remove the shelf.  

Follow the instructions in the *SAS Disk Shelves Service Guide* for your shelf model to hot-remove shelves.  

*NetApp Documentation: Disk Shelves* |
To remove a plex from a mirrored aggregate, you need to unmirror the aggregate.

### Scenario

### Steps

**a.** Identify the plex that you want to remove by using the `run -node local sysconfig -r` command.

In the following example, you can identify the plex from the line

```
Plex /dpg_mcc_8020_13_al_aggr1/plex0
```

In this case, the plex to specify is `plex0`.

```
dpgmcc_8020_13_al2::storage aggregate> run -node local sysconfig -r
*** This system has taken over dpg-mcc-8020-13-al
Aggregate dpg_mcc_8020_13_al_aggr1 (online, raid_dp, mirrored)
(block checksums)
Plex /dpg_mcc_8020_13_al_aggr1/plex0 (online, normal, active, pool0)
RAID group /dpg_mcc_8020_13_al_aggr1/plex0/rg0 (normal, block checksums)
```

**b.** Use the `storage aggregate plex delete -aggregate aggr_name -plex plex_name` command to remove the plex. `plex` defines the plex name, such as `plex3` or `plex6`.

**c.** Use the standard procedure to remove ownership of all drives in that shelf, and then physically remove the shelf.

Follow the instructions in the *SAS Disk Shelves Service Guide* for your shelf model to hot-remove shelves.

*NetApp Documentation: Disk Shelves*
Replacing a shelf nondisruptively in a fabric-attached MetroCluster configuration

You might need to know how to replace a shelf nondisruptively in a fabric-attached MetroCluster configuration.

About this task

Note: This procedure is only for use in a fabric-attached MetroCluster configuration.

Steps
1. Disabling access to the shelf on page 123
2. Replacing the shelf on page 126
3. Reenabling access and verifying the operation on page 126

Disabling access to the shelf

You must disable access to the shelf before you replace the shelf modules.

Before you begin

Check the overall health of the configuration. If the system does not appear healthy, address the issue first before proceeding.

Steps
1. Offline the affected plexes on the controller where they are hosted:
   
   \texttt{aggr offline plex\_name}

   Example
   
   The example shows the commands for offlining plexes for a controller running cMode.

   \begin{verbatim}
   Cluster\_A\_1::> storage aggregate plex offline -aggr aggr1 -plex plex2
   Cluster\_A\_1::> storage aggregate plex offline -aggr aggr2 -plex plex6
   Cluster\_A\_1::> storage aggregate plex offline -aggr aggr3 -plex plex1
   \end{verbatim}

2. Verify that the plexes are offline:
   
   \texttt{aggr status \textasciitilde aggr\_name}

   Example
   
   The example shows the commands for verifying that the aggregates are offline for a controller running cMode.

   \begin{verbatim}
   Cluster\_A\_1::> storage aggregate show -aggr aggr1
   Cluster\_A\_1::> storage aggregate show -aggr aggr2
   Cluster\_A\_1::> storage aggregate show -aggr aggr3
   \end{verbatim}

3. Disable the SAS ports or switch ports depending on whether the bridges connecting the target shelf are connecting a single SAS stack or two or more SAS stacks:
• If the bridges are connecting a single SAS stack, disable the switch ports that the bridges are connected to using the appropriate command for your switch.

The following example shows a pair of bridges that connect a single SAS stack, which contains the target shelf:

Switch ports 8 and 9 on each switch connect the bridges to the network.

The following example shows ports 8 and 9 being disabled on a Brocade switch.

```
FC_switch_A_1:admin> portDisable 8
FC_switch_A_1:admin> portDisable 9
FC_switch_A_2:admin> portDisable 8
FC_switch_A_2:admin> portDisable 9
```

The following example shows port 8 and 9 being disabled on a Cisco switch.

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# int fc1/8
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# int fc1/9
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# end

FC_switch_A_2# conf t
FC_switch_A_2(config)# int fc1/8
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# int fc1/9
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# end
```

• If the bridges are connecting two or more SAS stacks, disable the SAS ports connecting the bridges to the target shelf:

```
SASportDisable port number
```

**Note:** This is not applicable to FibreBridge 6500 bridges.

The following example shows a pair of bridges that connect four SAS stacks. SAS stack 2 contains the target shelf:
SAS port B connects the bridges to the target shelf. By disabling only SAS port B on both shelves, the other SAS stacks can continue to serve data during the replacement procedure. In this case, disable the SAS port connecting the bridge to the target shelf:

**SASportDisable port number**

The following example shows SAS port B being disabled from the bridge and also verifies that it is disabled. You must repeat the command on both bridges.

```
Ready.
SASPortDisable B
SAS Port B has been disabled.
```

4. If you previously disabled the switch ports, verify that they are disabled:

```
switchShow
```

**Example**

The example shows that the switch ports are disabled on a Brocade switch.

```
FC_switch_A_1:admin> switchShow
FC_switch_A_2:admin> switchShow
```

**Example**

The example shows that the switch ports are disabled on a Cisco switch.

```
FC_switch_A_1# show interface fc1/6
FC_switch_A_2# show interface fc1/6
```

5. Wait for ONTAP to realize that the disk is missing.

6. Power off the shelf that you want to replace.
Replacing the shelf

You must physically remove all of the cables and the shelf before inserting and cabling the new shelf and shelf modules.

Steps
1. Remove all disks and disconnect all cables from the shelf that is being replaced.
2. Remove the shelf modules.
3. Insert the new shelf.
4. Insert the new disks into the new shelf.
5. Insert the shelf modules.
6. Cable the shelf (SAS or Power).
7. Power on the shelf.

Reenabling access and verifying the operation

After the shelf has been replaced, you need to reenable access and verify that the new shelf is operating correctly.

Steps
1. Verify that the shelf powers properly and the links on the IOM modules are present.
2. Enable the switch ports or SAS port according to the following scenarios:

<table>
<thead>
<tr>
<th>Option</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you previously disabled</td>
<td>Enable the switch ports: <strong>portEnable</strong> port number</td>
</tr>
<tr>
<td>switch ports</td>
<td>a. The example shows the switch port being enabled on a Brocade switch.</td>
</tr>
</tbody>
</table>

```
Switch_A_1:admin> portEnable 6
Switch_A_2:admin> portEnable 6
```

b. The example shows the switch port being enabled on a Cisco switch.

```
Switch_A_1# conf t
Switch_A_1(config)# int fc1/6
Switch_A_1(config)# no shut
Switch_A_1(config)# end
Switch_A_2# conf t
Switch_A_2(config)# int fc1/6
Switch_A_2(config)# no shut
Switch_A_2(config)# end
```
<table>
<thead>
<tr>
<th>Option</th>
<th>Step</th>
</tr>
</thead>
</table>
| If you previously disabled a SAS port | **a.** Enable the SAS port connecting the stack to the shelf location:  

```bash
SASPortEnable port number
```

The example shows SAS port A being enabled from the bridge and also verifies that it is enabled.

```
Ready. *
SASPortEnable A
SAS Port A has been enabled.
```

**Note:** This is not applicable to ATTO 6500 FibreBridges.

3. If you previously disabled the switch ports, verify that they are enabled and online and that all devices are logged in correctly:

```bash
switchShow
```

**Example**

The example shows the `switchShow` command for verifying that a Brocade switch is online.

```
Switch_A_1:admin> SwitchShow
Switch_A_2:admin> SwitchShow
```

**Example**

The example shows the `switchShow` command for verifying that a Cisco switch is online.

```
Switch_A_1# show interface fc1/6
Switch_A_2# show interface fc1/6
```

**Note:** After several minutes, ONTAP detects that new disks have been inserted and displays a message for each new disk.

4. Verify that the disks have been detected by ONTAP:

```bash
sysconfig -a
```

5. Online the plexes that were offline earlier:

```bash
aggr online plex_name
```

**Example**

The example shows the commands for placing plexes on a controller running cMode back online.

```
Cluster_A_1::> storage aggregate plex online -aggr aggr1 -plex plex2
Cluster_A_1::> storage aggregate plex online -aggr aggr2 -plex plex6
Cluster_A_1::> storage aggregate plex online -aggr aggr3 -plex plex1
```

The plexes begin to resynchronize.

**Note:** You can monitor the progress of resynchronization using the `aggr status -r aggr_name` command.
When to migrate root volumes to a new destination

You might need to move root volumes to another root aggregate within a two-node or four-node MetroCluster configuration.

**Migrating root volumes within a two-node MetroCluster configuration**

To migrate root volumes to a new root aggregate within a two-node MetroCluster configuration, you should refer to the procedure in the following Knowledgebase answer. This procedure shows you how to non-disruptively migrate the root volumes during a MetroCluster switchover operation. This procedure is slightly different than the procedure used on a four-node configuration.

*NetApp Knowledgebase Answer 1030533: How to move mroot to a new root aggregate in a 2-node Clustered MetroCluster with Switchover*

**Migrating root volumes within a four-node MetroCluster configuration**

To migrate root volumes to a new root aggregate within a four-node MetroCluster configuration, you can use the `system node migrate-root` command while meeting the following requirements.

- You can use system node migrate-root to move root aggregates within a four-node MetroCluster configuration.
- All root aggregates must be mirrored.
- You can add new shelves on both sites with smaller SSDs to host the root aggregate.
- You must check the SSD limits that the platform supports before attaching new disks.
  *NetApp Hardware Universe*
- If you move the root aggregate to smaller disks, you need to accommodate the minimum root volume size of the platform to ensure all core files are saved.

*Note:* The four-node procedure can also be applied to an eight-node configuration.
Moving a metadata volume in MetroCluster configurations

You can move a metadata volume from one aggregate to another aggregate in a MetroCluster configuration. You might want to move a metadata volume when the source aggregate is decommissioned or unmirrored, or for other reasons that make the aggregate ineligible.

Before you begin

- You must have cluster administrator privileges to perform this task.
- The target aggregate must be mirrored and should not be in the degraded state.
- The available space in the target aggregate must be larger than the metadata volume that you are moving.

Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Identify the metadata volume that should be moved:
   ```
   volume show MDV_CRS*
   ```
   Example
   ```
   Cluster_A::*> volume show MDV_CRS*
   Vserver   Volume       Aggregate    State      Type       Size  Available Used%
   --------- ------------ ------------ ---------- ---- ---------- ---------- -----
   Cluster_A MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
   Node_A_1_aggr1 online RW 10GB     9.50GB    5%
   Cluster_A MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
   Node_A_2_aggr1 online RW 10GB     9.50GB    5%
   Cluster_A MDV_CRS_15035e66c9f311e7902700a098439625_A
   Node_B_1_aggr1 - RW      - - -
   Cluster_A MDV_CRS_15035e66c9f311e7902700a098439625_B
   Node_B_2_aggr1 - RW      - - -
   4 entries were displayed.
   Cluster_A::>
   ```

3. Identify an eligible target aggregate:
   ```
   metrocluster check config-replication show-aggregate-eligibility
   ```
   Example
   The following command identifies the aggregates in cluster_A that are eligible to host metadata volumes:
   ```
   Cluster_A::** metrocluster check config-replication show-aggregate-eligibility
   Aggregate Hosted Config Replication Vols Host Addl Vols Comments
   ----------------- ------------------------------------------ -------------- --------
   Node_A_1_aggr0   false Root Aggregate
   Node_A_2_aggr0   false Root Aggregate
   Node_A_1_aggr1   MDV_CRS_1bc7134a5dddf11e3b63f123478563412_A true
   Node_A_2_aggr1   MDV_CRS_1bc7134a5dddf11e3b63f123478563412_B true
   Node_A_1_aggr2   true
   Node_A_2_aggr2   true
   Node_A_1_Aggr3   false Unable to determine available space of aggregate
   ```
4. Start the volume move operation:

```
volume move start -vserver svm_name -volume metadata_volume_name -destination-aggregate destination_aggregate_name
```

**Example**

The following command moves metadata volume MDV_CRS_14c00d4ac9f311e7922800a0984395f1 from aggregate Node_A_1_aggr1 to aggregate Node_A_1_aggr2:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume MDV_CRS_14c00d4ac9f311e7922800a0984395f1 -destination-aggregate aggr_cluster_A_02_01
```

Warning: You are about to modify the system volume "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A". This may cause severe performance or stability problems. Do not proceed unless directed to do so by support. Do you want to proceed? {y|n}: y

[Job 109] Job is queued: Move "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver "svm_cluster_A" to aggregate "aggr_cluster_A_02_01".

Use the "volume move show -vserver svm_cluster_A -volume MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status of this operation.

5. Verify the state of the volume move operation:

```
volume move show -volume vol_constituent_name
```

6. Return to the admin privilege level:

```
set -privilege admin
```
Renaming a cluster in MetroCluster configurations

Renaming a cluster in a MetroCluster configuration involves making the changes, and then verifying on both the local and remote clusters that the change took effect correctly.

Steps
1. View the cluster names using the
   `metrocluster node show` command:

   **Example**
   
   ```
   cluster_1::*> metrocluster node show
   DR Group Cluster Node               Configuration State  DR Mirroring Mode
   ----- ------ ------------------ -------------- --------- ---------------------
   1     cluster_1
   node_A_1           configured     enabled   normal
   node_A_2           configured     enabled   normal
   cluster_2
   node_B_1           configured     enabled   normal
   node_B_2           configured     enabled   normal
   4 entries were displayed.
   ```

2. Rename the cluster:
   `cluster identity modify -name new_name`

   **Example**
   
   In the following example, the `cluster_1` cluster is renamed `cluster_A`:
   ```
   cluster_1::*> cluster identity modify -name cluster_A
   ```

3. Verify on the local cluster that the renamed cluster is running normally:
   `metrocluster node show`

   **Example**
   
   In the following example, the newly renamed `cluster_A` is running normally:
   ```
   cluster_A::*> metrocluster node show
   DR Group Cluster Node               Configuration State  DR Mirroring Mode
   ----- ------ ------------------ -------------- --------- ---------------------
   1     cluster_A
   node_A_1           configured     enabled   normal
   node_A_2           configured     enabled   normal
   cluster_2
   node_B_1           configured     enabled   normal
   node_B_2           configured     enabled   normal
   4 entries were displayed.
   ```

4. Rename the remote cluster:
   `cluster peer modify-local-name -name cluster_2 -new-name cluster_B`

   **Example**
   
   In the following example, `cluster_2` is renamed `cluster_B`: 
5. Verify on the remote cluster that the local cluster was renamed and is running normally:

```
metrocluster node show
```

**Example**

In the following example, the newly renamed `cluster_B` is running normally:

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

<table>
<thead>
<tr>
<th>DR Group</th>
<th>Cluster</th>
<th>Node</th>
<th>Configuration</th>
<th>State</th>
<th>Mirroring</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cluster_B</td>
<td>node_B_1</td>
<td>configured</td>
<td>enabled</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>node_B_2</td>
<td>configured</td>
<td>enabled</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>cluster_A</td>
<td>configured</td>
<td>enabled</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>node_A_1</td>
<td>configured</td>
<td>enabled</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>node_A_2</td>
<td>configured</td>
<td>enabled</td>
<td>normal</td>
<td></td>
</tr>
</tbody>
</table>

4 entries were displayed.

6. Repeat these steps for each cluster that you want to rename.
Powering off and powering on a data center

You must know how to power off and power on a data center for the purpose of site maintenance or to relocate a site to another location.

About this task

If a site needs to be relocated and reconfigured (if you need to expand from a four-node to an eight-node cluster, for example), these tasks cannot be completed at the same time. This procedure only covers the steps that are required to perform site maintenance or to relocate a site without changing its configuration.

Note: This procedure is for use in both MetroCluster IP and FC configurations.

Powering off a MetroCluster site

You must power off a site and all of the equipment before site maintenance or relocation can begin.

Steps

1. Before you begin, check that any non-mirrored aggregates at the site are offline.

2. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:
      
      ```bash
      node run -node (node name) sysconfig -a
      ```
   b. Check for any health alerts on both clusters:
      
      ```bash
      system health alert show
      ```
   c. Confirm the MetroCluster configuration and that the operational mode is normal:
      
      ```bash
      metrocluster show
      ```
   d. Perform a MetroCluster check:
      
      ```bash
      metrocluster check run
      ```
   e. Display the results of the MetroCluster check:
      
      ```bash
      metrocluster check show
      ```
   f. Run Config Advisor.
      
      
      "NetApp Downloads: Config Advisor"
      
   g. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

3. Enter the following command to implement the switchover:

   ```bash
   metrocluster switchover
   ```

   The operation can take several minutes to complete.

   Attention:

   In MetroCluster FC configurations, the unmirrored aggregates will only be online after a switchover if the remote disks in the aggregate are accessible. If the ISLs fail, the local node

   ```bash
   Attention:
   ```
may be unable to access the data in the unmirrored remote disks. The failure of an aggregate can lead to a reboot of the local node.

4. Monitor and verify the completion of the switchover:

   `metrocluster operation show`

   **Example**

   ```
   cluster_A::*> metrocluster operation show
   Operation: Switchover
   Start time: 10/4/2012 19:04:13
   State: in-progress
   End time: -
   Errors: -
   ```

   ```
   cluster_A::*> metrocluster operation show
   Operation: Switchover
   Start time: 10/4/2012 19:04:13
   State: successful
   End time: 10/4/2012 19:04:22
   Errors: -
   ```

5. Identify and move offline the affected plexes that are located at the disaster site.

   **Note:** This step is only required in MetroCluster FC configurations. In MetroCluster IP configurations, the plexes are placed offline during the switchover.

   Non-mirrored plexes consisting of disks located at the disaster site are moved offline and become inaccessible. Failure to move the non-mirrored plexes that are located at the disaster site offline might result in an outage.

   **Example**

   a. Identify the affected plexes.

   Plexes that are owned by nodes at the surviving site consist of Pool1 disks. Plexes that are owned by nodes at the disaster site consist of Pool0 disks.

   **Note:** “Home” refers to the “home” owner, not the “current” owner.

   ```
   Cluster_A::> storage aggregate plex show -fields aggregate,status,is-online,Plex,pool
   aggregate    plex  status        is-online pool
   ------------ ----- ------------- --------- ----
   Node_B_1_aggr0 plex0 normal,active true     0
   Node_B_1_aggr0 plex1 normal,active true     1
   Node_B_2_aggr0 plex0 normal,active true     0
   Node_B_2_aggr0 plex5 normal,active true     1
   Node_B_1_aggr1 plex0 normal,active true     0
   Node_B_1_aggr1 plex3 normal,active true     1
   Node_B_2_aggr1 plex0 normal,active true     0
   Node_B_2_aggr1 plex1 normal,active true     1
   Node_A_1_aggr0 plex0 normal,active true     0
   Node_A_1_aggr0 plex4 normal,active true     1
   Node_A_1_aggr1 plex0 normal,active true     0
   Node_A_1_aggr1 plex4 normal,active true     1
   Node_A_2_aggr0 plex0 normal,active true     0
   Node_A_2_aggr0 plex4 normal,active true     1
   Node_A_2_aggr1 plex0 normal,active true     0
   Node_A_2_aggr1 plex1 normal,active true     1
   14 entries were displayed.
   ```

   The affected plexes are those that are remote to cluster A. The following table shows whether the disks are local or remote relative to cluster A:
<table>
<thead>
<tr>
<th>Node</th>
<th>Disks in pool</th>
<th>Should the disks be set offline?</th>
<th>Example of plexes to be moved offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node _A_1 and Node _A_2</td>
<td>Disks in pool 0</td>
<td>No. Disks are local to cluster A.</td>
<td>-</td>
</tr>
</tbody>
</table>
|                      | Disks in pool 1 | Yes. Disks are remote to cluster A. | Node_A_1_aggr0/plex4  
Node_A_1_aggr1/plex1  
Node_A_2_aggr0/plex4  
Node_A_2_aggr1/plex1 |
| Node _B_1 and Node _B_2 | Disks in pool 0 | Yes. Disks are remote to cluster A. | Node_B_1_aggr1/plex0  
Node_B_1_aggr0/plex0  
Node_B_2_aggr0/plex0  
Node_B_2_aggr1/plex0 |
|                      | Disks in pool 1 | No. Disks are local to cluster A. | -                                    |

b. Move the affected plexes offline:

```
storage aggregate plex offline
```

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

**Note:** Perform this for all plexes that have disks that are remote to Cluster A.

6. Persistently offline the switchports according to the switch type.

**Note:** This step is only required for MetroCluster FC configurations. Skip this step if your configuration is a MetroCluster IP configuration or a stretched MetroCluster configuration with FC backend switches.
Switch type | Action
--- | ---
If the FC switches are Brocade switches... | a. Use the `portpersistentdisable port` command to persistently disable the ports as shown in the following example. This must be done on both switches at the surviving site.

```
Switch_A_1:admin> portpersistentdisable 14
Switch_A_1:admin> portpersistentdisable 15
Switch_A_1:admin>
```

b. Verify that the ports are disabled using the `switchshow` command shown in the following example:

```
Switch_A_1:admin> switchshow
switchName: Switch_A_1
switchType: 109.1
switchState: Online
switchMode: Native
switchRole: Principal
switchDomain: 2
switchId: fffc02
switchWwn: 10:00:00:05:33:88:9c:68
zoning: ON (T5_T6)
switchBeacon: OFF
FC Router: OFF
FC Router BB Fabric ID: 128
Address Mode: 0
Index Port Address Media Speed State Proto
==============================================
... 14 14 020e00 id 16G No_Light FC Disabled (Persistent)
... 15 15 020f00 id 16G No_Light FC Disabled (Persistent)
Switch_A_1:admin>
```

If the FC switches are Cisco switches... | a. Use the `interface` command to persistently disable the ports. The following example shows ports 14 and 15 being disabled:

```
Switch_A_1# conf t
Switch_A_1(config)# interface fc1/14-15
Switch_A_1(config)# shut
Switch_A_1(config-if)# end
Switch_A_1# copy running-config startup-config
```

b. Verify that the switch port is disabled using the `show interface brief` command as shown in the following example:

```
Switch_A_1# show interface brief
Switch_A_1
```

7. Power off the site.

The following equipment needs to be turned off in no specific order:

<table>
<thead>
<tr>
<th>Configuration type</th>
<th>Equipment to be powered off</th>
</tr>
</thead>
<tbody>
<tr>
<td>In a MetroCluster IP configuration, power off...</td>
<td>• MetroCluster IP switches</td>
</tr>
<tr>
<td></td>
<td>• Storage controllers</td>
</tr>
<tr>
<td></td>
<td>• Storage shelves</td>
</tr>
</tbody>
</table>
In a MetroCluster FC configuration, power off...
- MetroCluster FC switches
- Storage controllers
- Storage shelves
- Atto FibreBridges (if present)

Relocating the powered-off site of the MetroCluster

Once the site is powered off, you can begin maintenance work. The procedure is the same whether the MetroCluster components are relocated within the same data center or relocated to a different data center.

About this task
- The hardware should be cabled in the same way as the previous site.
- If the Inter-Switch Link (ISL) speed, length, or number has changed, they all need to be reconfigured.

Steps
1. Make sure that the cabling for all components is carefully recorded so that it can be correctly reconnected at the new location.
2. Physically relocate all the hardware, storage controllers, FC and IP switches, FibreBridges, and storage shelves.
3. Configure the ISL ports and verify the intersite connectivity.
   a. Power on the FC and IP switches.
      
      Note: Do not power up any other equipment.
4. Enable the ports.
   
   Note: This step is only required in MetroCluster FC configurations. You can skip this step if your configuration is a MetroCluster IP configuration.

Enable the ports according to the correct switch types in the following table:
Switch type

If the FC Switches are Brocade switches...

a. Use the `portcfgpersistentenable port number` command to persistently enable the port. This must be done on both switches at the surviving site.

The following example shows ports 14 and 15 being enabled on Switch_A_1.

```
switch_A_1:admin> portcfgpersistentenable 14
switch_A_1:admin> portcfgpersistentenable 15
switch_A_1:admin>
```

b. Verify that the switch port is enabled: `switchshow`

The following example shows that ports 14 and 15 are enabled:

```
switch_A_1:admin> switchshow
switchName:    Switch_A_1
switchType:    109.1
switchState:    Online
switchMode:    Native
switchRole:    Principal
switchDomain:    2
switchId:    fffc02
switchWwn:    10:00:00:05:33:88:9c:68
zoning:        ON (T5_T6)
switchBeacon:    OFF
FC Router:    OFF
FC Router BB Fabric ID:    128
Address Mode:    0

Index Port Address Media Speed State     Proto
==============================================
... 14  14   020e00   id    16G   Online      FC  E-Port
10:00:00:05:33:86:89:cb "Switch_A_1" 15  15   020f00   id    16G   Online      FC  E-Port
10:00:00:05:33:86:89:cb "Switch_A_1" (downstream)
... switch_A_1:admin>
```

If the FC Switches are Cisco switches...

a. Enter the `interface` command to enable the port.

The following example shows ports 14 and 15 being enabled on Switch_A_1.

```
switch_A_1# conf t
switch_A_1(config)# interface fc1/14-15
switch_A_1(config)# no shut
switch_A_1(config-if)# end
switch_A_1# copy running-config startup-config
```

b. Verify that the switch port is enabled: `show interface brief`

```
switch_A_1# show interface brief
switch_A_1#
```

5. Use tools on the switches (as they are available) to verify the intersite connectivity.

**Note:** You should only proceed if the links are properly configured and stable.

6. Disable the links again if they are found to be stable.

Disable the ports based on whether you are using Brocade or Cisco switches as shown in the following table:
If the FC Switches are Brocade switches...

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Enter the <code>portcfgpersistentdisable port number</code> command to persistently disable the port. This must be done on both switches at the surviving site. The following example shows ports 14 and 15 being disabled on Switch_A_1:</td>
<td></td>
</tr>
</tbody>
</table>
| `switch_A_1:admin> portpersistentdisable 14`
| `switch_A_1:admin> portpersistentdisable 15` |
| b. Verify that the switch port is disabled: **switchshow** The following example shows that ports 14 and 15 are disabled: |
| `switch_A_1:admin> switchshow`
| `switchName:    Switch_A_1`
| `switchType:    109.1`
| `switchState:   Online`
| `switchMode:    Native`
| `switchRole:    Principal`
| `switchDomain:  2`
| `switchId:      fffc02`
| `switchWwn:     10:00:00:05:33:88:9c:68`
| `zoning:        ON (T5_T6)`
| `switchBeacon:  OFF`
| `FC Router:     OFF`
| `FC Router BB Fabric ID:  128`
| `Address Mode:  0`
| `Index Port Address Media Speed State     Proto-------------------------------`
| `... 14 14 020e00   id    16G   No_Light    FC  Disabled (Persistent)`
| `15 15 020f00   id    16G   No_Light    FC  Disabled (Persistent)`
| `...` |

If the FC Switches are Cisco switches...

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Disable the port using the <strong>interface</strong> command. The following example shows ports fc1/14 and fc1/15 being disabled on Switch_A_1:</td>
<td></td>
</tr>
</tbody>
</table>
| `switch_A_1# conf t`
| `switch_A_1(config)# interface fc1/14-15`
| `switch_A_1(config)# shut`
| `switch_A_1(config-if)# end`
| `switch_A_1# copy running-config startup-config` |
| b. Verify that the switch port is disabled using the **show interface brief** command. |
| `switch_A_1# show interface brief`
| `switch_A_1#` |
Reestablishing the MetroCluster configuration and returning to normal operation

After maintenance has been completed or the site has been moved, you must power on the site and reestablish the MetroCluster configuration.

Steps

1. Power on the switches.
   Switches should be powered on first. They might have been powered on during the previous step if the site was relocated.
   a. Reconfigure the Inter-Switch Link (ISL) if required or if this was not completed as part of the relocation.
   b. Enable the ISL if fencing was completed.
   c. Verify the ISL.

2. Power on the shelves and allow enough time for them to power on completely.

3. Power on the FibreBridge bridges.
   **Note:** You can skip this step if your configuration is a MetroCluster IP configuration.
   a. On the FC switches, verify that the ports connecting the bridges are coming online.
      You can use a command such as `switchshow` for Brocade switches, and `show interface brief` for Cisco switches.
   b. Verify that the shelves and disks on the bridges are clearly visible.
      You can use a command such as `sastargets` on the ATTO command-line interface (CLI).

4. Enable the ISLs on the FC switches.
   **Note:** Skip this step if your configuration is a MetroCluster IP configuration.
   Enable the ports based on whether you are using Brocade or Cisco switches as shown in the following table:
If the FC Switches are Brocade switches...

**a.** Enter the `portcfgpersistentenable port` command to persistently enable the ports. This must be done on both switches at the surviving site.

The following example shows ports 14 and 15 being enabled on `Switch_A_1`:

```
Switch_A_1:admin> portcfgpersistentenable 14
Switch_A_1:admin> portcfgpersistentenable 15
Switch_A_1:admin>
```

**b.** Verify that the switch port is enabled using the `switchshow` command:

```
switch_A_1:admin> switchshow
switchName:    Switch_A_1
switchType:    109.1
switchState:    Online
switchMode:    Native
switchRole:    Principal
switchDomain:    2
switchId:    fffc02
switchWwn:    10:00:00:05:33:88:9c:68
zoning:        ON (T5_T6)
switchBeacon:    OFF
FC Router:    OFF
FC Router BB Fabric ID:    128
Address Mode:    0
Index Port Address Media Speed State     Proto
==============================================
... 14  14   020e00   id    16G   Online      FC  E-Port
10:00:00:05:33:86:89:cb "Switch_A_1"  
15  15   020f00   id    16G   Online      FC  E-Port
10:00:00:05:33:86:89:cb "Switch_A_1" (downstream)
...  
switch_A_1:admin>
```

If the FC Switches are Cisco switches...

**a.** Use the `interface` command to enable the ports.

The following example shows port fc1/14 and fc1/15 being enabled on `Switch_A_1`:

```
switch_A_1# conf t
switch_A_1(config)# interface fc1/14-15
switch_A_1(config)# no shut
switch_A_1(config-if)# end
switch_A_1# copy running-config startup-config
```

**b.** Verify that the switch port is disabled:

```
switch_A_1# show interface brief
switch_A_1#
```

5. Verify that the storage is now visible.

Select the appropriate method of determining whether the storage is visible based on whether you have a MetroCluster IP or FC configuration:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your configuration is a MetroCluster IP...</td>
<td>Verify that the local storage is visible from the node Maintenance mode.</td>
</tr>
</tbody>
</table>
6. Reestablish the MetroCluster configuration.

   Follow the instructions in the *MetroCluster Disaster and Recovery Guide* to perform healing and switchback operations according to your MetroCluster configuration.
Expanding a two-node MetroCluster FC configuration to a four-node configuration

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

Before you begin

- The nodes must be running ONTAP 9 or later in a MetroCluster FC configuration. This procedure is not supported on earlier versions of ONTAP or in MetroCluster IP configurations.
- If the platforms in your two-node configuration are not supported in ONTAP 9.2 and you plan to upgrade to platforms supported in ONTAP 9.2 and expand to a four-node cluster, you must upgrade the platforms in the two-node configuration before expanding the MetroCluster FC configuration.
- The existing MetroCluster FC configuration must be healthy.
- The equipment you are adding must be supported and meet all of the requirements described in the Fabric-attached MetroCluster Installation and Configuration Guide or the Stretch Installation and Configuration Guide.
- You must have available FC switch ports to accommodate the new controllers and any new bridges.
- You need the admin password and access to an FTP or SCP server.

About this task

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

![Diagram of MetroCluster FC configuration](attachment:image)

After completing this procedure, the MetroCluster FC configuration consists of two HA pairs, one at each site:
• Both sites must be expanded equally. A MetroCluster configuration cannot consist of an uneven number of nodes.

• This procedure can take over an hour per site, with additional time needed to initialize the disks. The time to initialize the disks depends on the size of the disks.

• This procedure uses the following workflow:
Steps
1. Verifying the state of the MetroCluster configuration on page 145
2. Sending a custom AutoSupport message before adding nodes to the MetroCluster configuration on page 147
3. Zoning for the new controller ports when adding a controller module in a fabric-attached MetroCluster configuration on page 147
4. Adding a new controller module to each cluster on page 147
5. Refreshing the MetroCluster configuration with new controllers on page 173
6. Enabling storage failover on both controller modules and enabling cluster HA on page 175
7. Restarting the SVMs on page 175

Verifying the state of the MetroCluster configuration
You should identify the existing controllers and confirm the disaster recovery (DR) relationships between them, that the controllers are in normal mode, and that the aggregates are mirrored.

Steps
1. Display the details of the nodes in the MetroCluster configuration from any node in the configuration:
   
   metrocluster node show -fields node,dr-partner,dr-partner-systemid
Example

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

```
cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-systemid
dr-group-id  cluster         node            dr-partner      dr-partner-systemid
-----------  -------------   -------         ----------      -------------------
1            cluster_A       controller_A_1  controller_B_1  536946192
1            cluster_B       controller_B_1  controller_A_1  536946165
2 entries were displayed.
```

2. Display the state of the MetroCluster configuration:

```
metrocluster show
```

Example

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

```
cluster_A::> metrocluster show
Configuration: two-node-fabric
Cluster                        Entry Name             State
------------------------------ ---------------------- ---------------------
Local: cluster_A               Configuration State    configured
                   Mode                   normal
               AUSO Failure Domain    auso-on-cluster-disaster
Remote: controller_B_1_siteB
Configuration State    configured
                   Mode                   normal
               AUSO Failure Domain    auso-on-cluster-disaster
```

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

```
storage aggregate show
```

Example

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

```
cluster_A::> storage aggregate show
Aggregate                Size     Available Used%  State   #Vols  Nodes            RAID  Status
---------                -------- --------- -----  ------- ------ ----------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1    controller_A_1
raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2    controller_A_1
raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1    controller_A_1
raid_dp,mirrored
3 entries were displayed.
```
Sending a custom AutoSupport message before adding nodes to the MetroCluster configuration

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

**About this task**

This task must be performed on each MetroCluster site.

**Steps**

1. Log in to the cluster at Site_A.
2. Invoke an AutoSupport message indicating the start of the maintenance:
   
   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```
   
   `maintenance-window-in-hours` specifies the length of the maintenance window and can be a maximum of 72 hours. If you complete the maintenance before the time has elapsed, you can issue the
   
   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

   3. Repeat this step on the partner site.

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

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

**About this task**

If you manually configured your FC switches, you must ensure that the zoning is correct for the initiator connections from the new controller modules. See the sections on zoning in the Fabric-attached MetroCluster Installation and Configuration Guide.

*Fabric-attached MetroCluster installation and configuration*

Adding a new controller module to each cluster

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

**Before you begin**

- The new controller module must be received from NetApp as part of the upgrade kit.
  
  You should verify that PCIe cards in the new controller module are compatible and supported by the new controller module.

*NetApp Hardware Universe*
• Your system must have an empty slot available for the new controller module when upgrading to a single-chassis HA pair (an HA pair in which both controller modules reside in the same chassis).
  
  **Note:** This configuration is not supported on all systems.

• You must have rack space and cables for the new controller module when upgrading to a dual-chassis HA pair (an HA pair in which the controller modules reside in separate chassis).
  
  **Note:** This configuration is not supported on all systems.

• Each controller module must be connected to the management network through its e0a port or, if your system has one, the e0M port (wrench port).

**About this task**

• These tasks must be repeated at each site.

• The preexisting controller modules are referred to as the *existing* controller modules. The examples in this procedure have the console prompt `existing_ctlr>`.

• The controller modules that are being added are referred to as the *new* controller modules; the examples in this procedure have the console prompt `new_ctlr>`.

• This task uses the following workflow:
Steps

1. Preparing for the upgrade on page 150
2. Preparing cluster ports on an existing controller module on page 151
3. Preparing the netboot server to download the image on page 153
4. Setting the HA mode on the existing controller module on page 154
5. Shutting down the existing controller module on page 154
6. Installing and cabling the new controller module on page 155
7. Powering up both controller modules and displaying the LOADER prompt on page 157
8. Configuring and cabling CNA ports (80xx systems only) on page 158
Preparing for the upgrade

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

Steps

1. Verify that your system has enough available disks for the new controller module.

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

   *Physical Storage Management Guide*

   *Disk and aggregate management*

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

<table>
<thead>
<tr>
<th>If the result showed...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enough spare disks available for the new controller module</td>
<td>Go to the next step.</td>
</tr>
<tr>
<td>Not enough spares for the new controller module on a system without root-data partitioning</td>
<td>Complete the following substeps:</td>
</tr>
<tr>
<td></td>
<td>a. Determine where the aggregates for the existing node are located:</td>
</tr>
<tr>
<td></td>
<td><em>storage aggregate show</em></td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> If you do not have enough free disks for your system, you need to add more storage. Contact technical support for more information.</td>
</tr>
<tr>
<td></td>
<td>b. If disk ownership automatic assignment is on, turn it off:</td>
</tr>
<tr>
<td></td>
<td><em>storage disk option modify -node node_name -autoassign off</em></td>
</tr>
<tr>
<td></td>
<td>c. Remove ownership on disks that do not have aggregates on them:</td>
</tr>
<tr>
<td></td>
<td><em>storage disk removeowner disk_name</em></td>
</tr>
<tr>
<td></td>
<td>d. Repeat the previous step for as many disks as you need for the new node.</td>
</tr>
</tbody>
</table>

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

   - Cluster connections

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

- HA interconnect connections, if the system is in a dual-chassis HA pair
- Storage connections to the FC switches
- Cluster peering connections

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

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

NetApp Hardware Universe

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

Preparing cluster ports on an existing controller module

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

About this task

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

For detailed information about port, LIF, and network configuration in ONTAP, see the Network Management Guide.

Steps

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

   For a list of the default port roles for your platform, see the Hardware Universe at hwu.netapp.com

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

2. For each cluster port, identify the port roles: `network port show`

Example

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

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

<table>
<thead>
<tr>
<th>Speed(Mbps)</th>
<th>Health</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>e0M</td>
<td>Default</td>
<td>mgmt_bd_1500</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0a</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0b</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0i</td>
<td>Default</td>
<td>down</td>
<td>1500</td>
<td>auto/10</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0j</td>
<td>Default</td>
<td>down</td>
<td>1500</td>
<td>auto/10</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0k</td>
<td>Default</td>
<td>down</td>
<td>1500</td>
<td>auto/10</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e0l</td>
<td>Default</td>
<td>down</td>
<td>1500</td>
<td>auto/10</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e2a</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e2b</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e4a</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e4b</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/10000</td>
<td>healthy</td>
<td></td>
</tr>
</tbody>
</table>

13 entries were displayed.

3. If the port roles are not set to `cluster`: 
152 | MetroCluster Service and Expansion Guide

You must change each incorrect port role to the correct role:  
```
  network port broadcast-domain remove-ports -ipspace Default -broadcast-domain Default -ports node_name:port_name
```

**Note:** Your domain name might be different from the name that is shown in the example.

You must add the port to the cluster domain:  
```
  network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports node_name:port_name
```

4. Verify that the port roles have changed:  
```
  network port show
```

**Example**

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

<table>
<thead>
<tr>
<th>Node: controller_A_1</th>
<th>Speed(Mbps)</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>IPspace</td>
<td>Broadcast Domain</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>e0M</td>
<td>Default</td>
<td>mgmt_bd_1500</td>
</tr>
<tr>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
</tr>
<tr>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
</tr>
<tr>
<td>e0c</td>
<td>Cluster</td>
<td>Cluster</td>
</tr>
<tr>
<td>e0d</td>
<td>Cluster</td>
<td>Cluster</td>
</tr>
<tr>
<td>e0i</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e0j</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e0k</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e0l</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e2a</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e2b</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e4a</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>e4b</td>
<td>Default</td>
<td>Default</td>
</tr>
</tbody>
</table>

13 entries were displayed.

5. For each cluster port, change the home port of any of the data LIFs on that port to a data port:  
```
  network interface modify
```

**Example**

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

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

6. For each LIF that you modified, revert the LIF to its new home port:  
```
  network interface revert
```

**Example**

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

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

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

**Example**

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

```
cluster1::> network interface create -vserver Cluster -lif clus1 -role cluster -home-node node0 -home-port ela -auto true
```
8. If you are creating a two-node switchless cluster, enable the switchless cluster networking mode:
   a. Change to the advanced privilege level from either node: `set -privilege advanced`
      You can respond `y` when prompted whether you want to continue into advanced mode. The advanced mode prompt appears (>).
   b. Enable the switchless cluster networking mode: `network options switchless-cluster modify -enabled true`
   c. Return to the admin privilege level: `set -privilege admin`

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

**Related information**

*Network and LIF management*

**Preparing the netboot server to download the image**

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

**Before you begin**

- You must be able to access an HTTP server from the system before and after adding the new controller module.
- You must have access to the NetApp Support Site to download the necessary system files for your platform and your version of ONTAP.

**NetApp Support Site**

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

**Steps**

1. **Download and extract the netboot.tgz file from the NetApp Support Site.**
   
   The `netboot.tgz` file is used for performing a netboot of your system. You should download the file contents to a web-accessible directory.
   
   a. Download the `netboot.tgz` file from the NetApp Support Site to a web-accessible directory.
   b. Switch to the web-accessible directory.
   c. Extract the contents of the `netboot.tgz` file to the target directory:
      ```
      tar -zxvf netboot.tgz.
      ```
   
   Your directory listing should contain the following directory:

   ```
   netboot/
   ```

   **Note:** If you are extracting the contents using Windows, do not use winzip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

2. **Download the image.tgz file from the NetApp Support Site to the web-accessible directory.**
   
   Your directory listing should contain the following file and directory:
3. Determine the IP address of the existing controller module.
   This address is referred to later in this procedure as `ip-address-of-existing controller`.

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

### Setting the HA mode on the existing controller module

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

#### Step

1. Set the mode to HA:

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

### Shutting down the existing controller module

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

#### Steps

1. Halt the node from the existing controller module prompt: `halt local -inhibit-takeover true`

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

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

   - In a 32xx system, the NVMEM LED is located on the controller module to the right of the network ports, marked with a battery symbol.
   - In a 62xx system, the NVRAM LED is located on the controller module to the right of the network ports, marked with a battery symbol.
   - In an 80xx system, the NVRAM LED is located on the controller module to the right of the network ports, marked with a battery symbol.

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

2. If you are not already grounded, properly ground yourself.

3. Turn off the power supplies and disconnect the power, using the correct method for your system and power-supply type:

```
<table>
<thead>
<tr>
<th>If your system uses...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC power supplies</td>
<td>Unplug the power cords from the power source, and then remove the power cords.</td>
</tr>
<tr>
<td>DC power supplies</td>
<td>Remove the power at the DC source, and then remove the DC wires, if necessary.</td>
</tr>
</tbody>
</table>
```
Installing and cabling the new controller module

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

**Steps**

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

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

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

<table>
<thead>
<tr>
<th>If you are adding a controller module...</th>
<th>Then perform these steps...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To an empty bay to create a single-chassis HA pair and the system belongs to one of the following platforms:</td>
<td>a. Install three additional fans in the chassis to cool the new controller module:</td>
</tr>
<tr>
<td>• 6210</td>
<td>i. Remove the bezel by using both hands to hold it by the openings on each side, and then pull the bezel away from the chassis until it releases from the four ball studs on the chassis frame.</td>
</tr>
<tr>
<td>• 6220</td>
<td>ii. Remove the blank plate that covers the bay that will contain the new fans.</td>
</tr>
<tr>
<td></td>
<td>iii. Install the fans as described in the Replacing a fan module document for your system on the NetApp Support Site at mysupport.netapp.com.</td>
</tr>
<tr>
<td>a.</td>
<td>b. Remove the blank plate in the rear of the chassis that covers the empty bay that will contain the new controller module.</td>
</tr>
<tr>
<td></td>
<td>c. Gently push the controller module halfway into the chassis.</td>
</tr>
</tbody>
</table>

To an empty bay to create a single-chassis HA pair and the system belongs to one of the following platforms:

- AFF A700
- AFF A300
- FAS9000
- FAS8200
- 8020
- 8040
- 8060
- 32xx

a. Remove the blank plate in the rear of the chassis that covers the empty bay that will contain the new controller module.

b. Gently push the controller module halfway into the chassis.

To prevent the controller module from automatically booting, do not fully seat it in the chassis until later in this procedure.
If you are adding a controller module...

<table>
<thead>
<tr>
<th>In a separate chassis from its HA partner to create a dual-chassis HA pair when the existing configuration is in a controller-IOX module configuration.</th>
<th>Then perform these steps...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the new system in the rack or system cabinet.</td>
<td></td>
</tr>
</tbody>
</table>

- FAS32xx
- FAS62xx
- FAS8080

3. Cable the HA interconnect if you have a dual-chassis HA pair.

4. Cable the new FC-to-SAS bridges to the FC switches and the storage shelves.

The FC-to-SAS bridge configuration and port usage is described in the Fabric-attached MetroCluster Installation and Configuration Guide.

Fabric-attached MetroCluster installation and configuration

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

<table>
<thead>
<tr>
<th>Switch vendor</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade</td>
<td>switchshow</td>
</tr>
<tr>
<td>Cisco</td>
<td>show interface brief</td>
</tr>
</tbody>
</table>

6. Cable the cluster network connections, as necessary:

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

   AFF and FAS Documentation Center

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


c. Connect cables to the cluster ports:

<table>
<thead>
<tr>
<th>If the cluster is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A two-node switchless cluster</td>
<td>Directly connect the cluster ports on the existing controller module to the corresponding cluster ports on the new controller module.</td>
</tr>
<tr>
<td>A switched cluster</td>
<td>Connect the cluster ports on each controller to the ports on the cluster network switches identified in substep b.</td>
</tr>
</tbody>
</table>

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

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

Step

1. Cable the FC-VI ports and HBA ports, using the table for your configuration and switch model.

   - Port assignments for FC switches when using ONTAP 9.1 and later on page 224
Cabling the new controller module's cluster peering connections

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

About this task

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

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

Step

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

   Cluster peering can be done on dedicated ports or on data ports. Using dedicated ports provides higher throughput for the cluster peering traffic.

   Cluster and SVM peering express configuration

Powering up both controller modules and displaying the LOADER prompt

You power up both controller modules and interrupt the normal boot process on each to display the LOADER prompt.

Step

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

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

<table>
<thead>
<tr>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In separate chassis</td>
</tr>
<tr>
<td>a. Turn on the power supplies on the existing controller module.</td>
</tr>
<tr>
<td>b. Interrupt the boot process by pressing Ctrl-C.</td>
</tr>
<tr>
<td>c. Repeat these steps for the new controller module</td>
</tr>
</tbody>
</table>

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

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

### Configuring and cabling CNA ports (80xx systems only)

If you are adding a controller module to an 80xx system, you must check the configuration of the CNA ports on the new controller module and, if necessary, change the default port configuration to match the CNA port configuration of the existing controller module.

#### Before you begin

You must have the SFP+ modules for the CNA ports. If the ports are set to a 10 GbE personality, you can use twinax cables.

#### Steps

1. **Boot to Maintenance mode on the new node, if it is not in Maintenance mode, by entering** `halt` to go to the LOADER prompt.
   
   If you are running ONTAP 8.2.1 or later, enter `boot_ontap maint` at the LOADER prompt and enter `y` to continue when prompted.

2. **On the existing controller module console, check how the ports are currently configured:** `system node hardware unified-connect show`

   **Example**

   The system displays output similar to the following example:

   ```
   *node_name:* node_name::> system node hardware unified-connect show
    Node Adapter Current Current Pending Pending
    ---- ------- ------ ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- ------ ------- --------
Expanding a two-node MetroCluster FC configuration to a four-node configuration

<table>
<thead>
<tr>
<th>f-a</th>
<th>0e</th>
<th>fc</th>
<th>initiator</th>
<th>-</th>
<th>-</th>
<th>online</th>
</tr>
</thead>
<tbody>
<tr>
<td>f-a</td>
<td>0f</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>f-a</td>
<td>0g</td>
<td>cna</td>
<td>target</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>

4. If the current SFP+ module does not match the desired use, replace it with the correct SFP+ module.

5. If the current configuration does not match the existing node's configuration, change the configuration as required:

<table>
<thead>
<tr>
<th>If the desired use is for...</th>
<th>Then enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC initiator</td>
<td>uadmin modify -t initiator adapter_name</td>
</tr>
<tr>
<td>FC target</td>
<td>uadmin modify -t target adapter_name</td>
</tr>
<tr>
<td>Ethernet</td>
<td>uadmin modify -m cna adapter_name</td>
</tr>
</tbody>
</table>

**Note:** If you changed the port configuration, it will take effect when the new node is booted. To confirm the configuration change, you must verify the settings after the boot.

6. Cable the port.

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

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

**About this task**

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

**Steps**

1. Change the ha-config setting of the existing controller module:
   a. Halt the existing controller module, and then boot it to Maintenance mode: `haltboot_ontap maint`
   b. Display the ha-config setting of the existing controller module and chassis:
      `ha-config show`
      The ha-config setting is `mcc-2n` for all components because the controller module was in a two-node MetroCluster configuration.
   c. Change the ha-config setting of the existing controller module to `mcc`:
      `ha-config modify controller mcc`
   d. Change the ha-config setting of the existing chassis to `mcc`:
      `ha-config modify chassis mcc`
   e. Retrieve the system ID for the existing controller module:
      `sysconfig`
      Note the system ID. You need it when you set the partner ID on the new controller module.
   f. Exit Maintenance mode to return to the LOADER prompt:
      `exit`
2. Change the ha-config setting and retrieve the system ID of the new controller module:
   a. If the new controller module is not already in Maintenance mode, boot it to Maintenance mode: `boot_ontap maint`
   b. Change the ha-config setting of the new controller module to `mcc`:
      `ha-config modify controller mcc`
   c. Change the ha-config setting of the new chassis to `mcc`:
      `ha-config modify chassis mcc`
   d. Retrieve the system ID for the new controller module:
      `sysconfig`
      Note the system ID. You need it when you set the partner ID and assign disks to the new controller module.
   e. Exit Maintenance mode to return to the LOADER prompt:
      `exit`

**Setting the partner system ID for both controller modules**

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

**About this task**

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

**Steps**

1. On the existing controller module, set the partner system ID to that of the new controller module:
   `setenv partner-sysid sysID_of_new_controller`

2. On the new controller module, set the partner system ID to that of the existing controller module:
   `setenv partner-sysid sysID_of_existing_controller`

**Booting the existing controller module**

You must boot the existing controller module to ONTAP.

**Step**

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

**Assigning disks to the new controller module**

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

**Before you begin**

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

*Preparing for the upgrade* on page 150
About this task
These steps are performed on the existing controller module.

Steps
1. Assign the root disk to the new controller module:
   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```
   If your platform model uses the Advanced Drive Partitioning (ADP) feature, you must include the `-root true` parameter:
   ```
   storage disk assign -disk disk_name -root true -sysid new_controller_sysID -force true
   ```
2. Assign the remaining required disks to the new controller module by entering the following command for each disk:
   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```
3. Verify that the disk assignments are correct:
   ```
   storage disk show -partitionownership
   ```
4. After you finish assigning disks, halt the node to the LOADER prompt:
   ```
   halt
   ```

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

About this task
• This task starts at the LOADER prompt of the new controller module.
• This task includes initializing disks.
  The amount of time you need to initialize the disks depends on the size of the disks.
• The system automatically assigns two disks to the new controller module.
  *Disk and aggregate management*

Steps
1. At the LOADER prompt, configure the IP address of the new controller module based on DHCP availability:
<table>
<thead>
<tr>
<th>If DHCP is...</th>
<th>Then enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td><code>ifconfig e0M -auto</code></td>
</tr>
</tbody>
</table>
If DHCP is...

Then enter the following command...

| Not available | ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain |

*filer_addr* is the IP address of the storage system.

*netmask* is the network mask of the storage system.

*gateway* is the gateway for the storage system.

*dns_addr* is the IP address of a name server on your network.

*dns_domain* is the Domain Name System (DNS) domain name. If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL; you need only the server’s host name.

**Note:** Other parameters might be necessary for your interface. For details, use the `help ifconfig` command at the LOADER prompt.

---

2. At the LOADER prompt, enter the following command:

```
netboot http://path_to_web-accessible_directory/netboot/kernel
```

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

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

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

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

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

   **Example**

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

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

   **Example**

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

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

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

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

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

   a. Enter the node management LIF information on the console.

   ```
   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 cluster setup wizard.
   Any changes you made before quitting will be saved.
   To accept a default or omit a question, do not enter a value.
   This system will send event messages and weekly 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, please 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: 10.98.230.86
   Enter the node management interface netmask: 255.255.240.0
   Enter the node management interface default gateway: 10.98.224.1
   A node management interface on port e0c with IP address 10.98.230.86 has been created.
   This node has its management address assigned and is ready for cluster setup.
   ```
   b. Enter the node management LIF information on the console as shown in the following example:
   c. Manually enter the admin login ID when prompted to do so.
   d. Manually start the Cluster Setup wizard at the prompt:
   ```
   cluster setup
   ```
10. With the **Cluster Setup** wizard running, join the node to the cluster:

   ```
   join
   ```

   **Example**

   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`

11. Respond **yes** when prompted to set storage failover to HA mode.

   **Example**

   Non-HA mode, Reboot node to activate HA
   Warning: Ensure that the HA partner has started disk initialization before
   rebooting this node to enable HA.
   Do you want to reboot now to set storage failover (SFO) to HA mode?
   {yes, no} [yes]: `yes`

   Rebooting now

   After the node reboots, the Cluster Setup wizard displays the “Welcome to node setup” screen and prompts you to complete the node setup.

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

   **Example**

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

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

   The **Software Setup Guide** for your version of ONTAP contains additional details.

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

   **Example**

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

   ```
   cluster_A::> network interface create -vserver Cluster -lif clus1 -role cluster -home-node node_A_1 -home-port ela -auto true
   ```
15. After setup is complete, verify that the node is healthy and eligible to participate in the cluster:

```
cluster show
```

**Example**

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Health</th>
<th>Eligibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>node_A_2</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

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

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

```
network port show
```

**Example**

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Speed (Mb/s)</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>node_A_2</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14 entries were displayed.

**Related information**

*ONTAP 9 Software Setup Guide*

**Mirroring the root aggregate on the new controller**

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

**About this task**

This task must be performed on the new controller module.

**Step**

1. Mirror the root aggregate:

```
storage aggregate mirror aggr_name
```
Example

The following command mirrors the root aggregate for controller_A_1:

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

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

Configuring intercluster LIFs

You must create intercluster LIFs on ports used for communication between the MetroCluster partner clusters. You can use dedicated ports or ports that also have data traffic.

Choices

- Configuring intercluster LIFs on dedicated ports on page 166
- Configuring intercluster LIFs on shared data ports on page 168

Configuring intercluster LIFs on dedicated ports

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

Steps

1. List the ports in the cluster:

   `network port show`

   For complete command syntax, see the man page.

   Example

   The following example shows the network ports in `cluster01`:

   

<table>
<thead>
<tr>
<th>Mode</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Speed (Mbps)</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster01-01</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>cluster01-02</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
</tbody>
</table>

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

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

   For complete command syntax, see the man page.

   Example

   The following example shows that ports `e0e` and `e0f` have not been assigned LIFs:
3. Create a failover group for the dedicated ports:

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

   **Example**

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

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

4. Verify that the failover group was created:

   ```
   network interface failover-groups show
   ```

   For complete command syntax, see the man page.

   **Example**

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

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

   ```
   network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group
   ```

   For complete command syntax, see the man page.

   **Example**

   The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02` in the failover group `intercluster01`:
6. Verify that the intercluster LIFs were created:

```
network interface create -vserver cluster01 -lif cluster01_icl01 -role intercluster -home-node cluster01-01 -home-port e0e -address 192.168.1.201 -netmask 255.255.255.0 -failover-group intercluster01
```

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

For complete command syntax, see the man page.

**Example**

```
cluster01::> network interface show –role intercluster
Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01
cluster01_icl01   up/up      192.168.1.201/24   cluster01-01  e0e     true
cluster01_icl02   up/up      192.168.1.202/24   cluster01-02  e0f     true
```

7. Verify that the intercluster LIFs are redundant:

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

For complete command syntax, see the man page.

**Example**

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

```
cluster01::> network interface show -role intercluster –failover
Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01-01      cluster01-01_icl01 cluster01-01:e0e   local-only      intercluster01
Failed Targets:  cluster01-01:e0f
cluster01-01_icl02 cluster01-02:e0e   local-only      intercluster01
Failed Targets:  cluster01-02:e0f
```

Configuring intercluster LIFs on shared data ports

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

**Steps**

1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

**Example**

The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
               Node Port   IPspace   Broadcast Domain Link MTU Admin/Oper
------------- ------ ------------------ ------------- ------ --------------
cluster01-01    e0a   Cluster       Cluster       up  1500   auto/1000
2. Create intercluster LIFs on the system SVM:

```
network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask
```

For complete command syntax, see the man page.

**Example**

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01 -role intercluster -home-node cluster01-01 -home-port e0c -address 192.168.1.201 -netmask 255.255.255.0
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl02 -role intercluster -home-node cluster01-02 -home-port e0c -address 192.168.1.202 -netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

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

For complete command syntax, see the man page.

**Example**

```
cluster01::> network interface show -role intercluster
Logical Interface Status Network Address/Mask Current Is Node Port Home
-------- --------------- --------------------- ------------- ------- ----
cluster01 cluster01_icl01 up/up 192.168.1.201/24 cluster01-01 e0c true
cluster01_icl02 up/up 192.168.1.202/24 cluster01-02 e0c true
```

4. Verify that the intercluster LIFs are redundant:

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

For complete command syntax, see the man page.

**Example**

```
cluster01::> network interface show -role intercluster -failover
Logical Interface Home Failover Failover
-------- --------------- --------- ---------
cluster01 cluster01_icl01 cluster01-01:e0c local-only 192.168.1.201/24
Failover Targets: cluster01-01:e0c, cluster01-01:e0d
cluster01_icl02 cluster01-02:e0c local-only 192.168.1.201/24
Failover Targets: cluster01-02:e0c, cluster01-02:e0d
```
Creating a mirrored data aggregate on each node

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

Before you begin

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

About this task

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

Disk and aggregate management

Steps

1. Display a list of available spares:
   ```
   storage disk show -spare -owner node_name
   ```
2. Create the aggregate by using the `storage aggregate create -mirror true` command.
   ```
   If you are logged in to the cluster on the cluster management interface, you can create an aggregate on any node in the cluster. To ensure that the aggregate is created on a specific node, use the `-node` parameter or specify drives that are owned by that node.
   You can specify the following options:
   - Aggregate's home node (that is, the node that owns the aggregate in normal operation)
   - List of specific drives or array LUNs that are to be added to the aggregate
   - Number of drives to include
     
     **Note:** In the minimum supported configuration, in which a limited number of drives are available, you must use the force-small-aggregate option to allow the creation of a three disk RAID-DP aggregate.
     
     - Checksum style to use for the aggregate
     - Type of drives to use
     - Size of drives to use
     - Drive speed to use
     - RAID type for RAID groups on the aggregate
     - Maximum number of drives or array LUNs that can be included in a RAID group
     - Whether drives with different RPM are allowed
   
   For more information about these options, see the `storage aggregate create` man page.
Example

The following command creates a mirrored aggregate with 10 disks:

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

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

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

Installing licenses for the new controller module

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

About this task

For detailed information about licensing, see the knowledgebase article 3013749: Data ONTAP 8.2 Licensing Overview and References on the NetApp Support Site and the System Administration Reference.

Steps

1. If necessary, obtain license keys for the new node on the NetApp Support Site in the My Support section under Software licenses.
   If the site does not have the license keys you need, contact your sales or support representative.

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

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

   The `license_key` is 28 digits in length.

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

Creating unmirrored data aggregates

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

Before you begin

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

About this task

Attention:

In MetroCluster FC configurations, the unmirrored aggregates will only be online after a switchover if the remote disks in the aggregate are accessible. If the ISLs fail, the local node may be unable to access the data in the unmirrored remote disks. The failure of an aggregate can lead to a reboot of the local node.

Note: The unmirrored aggregates must be local to the node owning them.
• Drives and array LUNs are owned by a specific node; when you create an aggregate, all drives in that aggregate must be owned by the same node, which becomes the home node for that aggregate.

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

• The Disks and Aggregates Power Guide contains more information about mirroring aggregates.

Steps
1. Display a list of available spares:

   `storage disk show -spare -owner node_name`

2. Create the aggregate:

   `storage aggregate create`

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

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

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

Example
The following command creates a unmirrored aggregate with 10 disks:

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

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

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

Related information

`Disk and aggregate management`
Installing the firmware after adding a controller module

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

Step

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

   NetApp Downloads: System Firmware and Diagnostics

After you finish

If you have not already done so, repeat the tasks for adding a second controller module on the MetroCluster partner site.

Refreshing the MetroCluster configuration with new controllers

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

Steps

1. Refresh the MetroCluster configuration:
   a. Enter advanced privilege mode:
      
      set -privilege advanced
   b. Refresh the MetroCluster configuration:
      
      metrocluster configure -refresh true

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

   controller_A_1::*> metrocluster configure -refresh true
   [Job 726] Job succeeded: Configure is successful.

   c. Return to admin privilege mode:
      
      set -privilege admin

2. Verify the networking status on site A:

   network port show

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

   cluster_A::> network port show
   Node  Port  IPspace  Broadcast Domain  Link  MTU  Admin/Oper  Speed (Mbps)
   ------  ------  -----------  --------------  -----  ------  ----------  -------
   controller_A_1

Expanding a two-node MetroCluster FC configuration to a four-node configuration | 173
3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.

a. Verify the configuration from site A:

```
metrocluster show
```

**Example**

```
cluster_A::> metrocluster show

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Entry Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local: cluster_A</td>
<td>Configuration state configured</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
<td></td>
</tr>
<tr>
<td>Remote: cluster_B</td>
<td>Configuration state configured</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
<td></td>
</tr>
</tbody>
</table>
```

b. Verify the configuration from site B:

```
metrocluster show
```

**Example**

```
cluster_B::> metrocluster show

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Entry Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local: cluster_B</td>
<td>Configuration state configured</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
<td></td>
</tr>
<tr>
<td>Remote: cluster_A</td>
<td>Configuration state configured</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
<td></td>
</tr>
</tbody>
</table>
```

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

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

```
<table>
<thead>
<tr>
<th>dr-group-id</th>
<th>cluster</th>
<th>node</th>
<th>ha-partner</th>
<th>dr-cluster</th>
<th>dr-partner</th>
<th>dr-auxiliary</th>
<th>node-object-limit</th>
<th>automatic-uso</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>cluster_A</td>
<td>rha1-a1</td>
<td>node_A_2</td>
<td>cluster_B</td>
<td>node_R_1</td>
<td>node_R_2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>cluster_A</td>
<td>rha1-a2</td>
<td>node_A_1</td>
<td>cluster_B</td>
<td>node_R_2</td>
<td>node_R_1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

14 entries were displayed.
Enabling storage failover on both controller modules and enabling cluster HA

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

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

About this task
This task must be performed on each MetroCluster site.

Steps
1. Enable storage failover:
   
   `storage failover modify -enabled true -node existing-node-name`
   
   The single command enables storage failover on both controller modules.

2. Verify that storage failover is enabled:
   
   `storage failover show`
   
   Example
   
   The output should be similar to the following:

<table>
<thead>
<tr>
<th>Node</th>
<th>Partner</th>
<th>Possible</th>
<th>State Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>old-ctlr</td>
<td>new-ctlr</td>
<td>true</td>
<td>Connected to new-ctlr</td>
</tr>
<tr>
<td>new-ctlr</td>
<td>old-ctlr</td>
<td>true</td>
<td>Connected to old-ctlr</td>
</tr>
</tbody>
</table>

3. Enable cluster HA:
   
   `cluster ha modify -configured true`
   
   Cluster high availability (HA) must be configured in a cluster if it contains only two nodes and it differs from the HA provided by storage failover.

Restarting the SVMs

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

Steps
1. Identify the SVMs that need to be restarted:
   
   `metrocluster vserver show`
   
   This command shows the SVMs on both MetroCluster clusters.
2. Restart the SVMs on the first cluster:
   a. Enter advanced privilege mode, pressing $y$ when prompted:
      
      ```
      set -privilege advanced
      ```
   
   b. Restart the SVMs:
      
      ```
      vserver start -vserver SVM_name -force true
      ```
   
   c. Return to admin privilege mode:
      
      ```
      set -privilege admin
      ```

3. Repeat the previous step on the partner cluster.

4. Verify that the SVMs are in a healthy state:
   
   ```
   metrocluster vserver show
   ```
Expanding a four-node MetroCluster FC configuration to an eight-node configuration

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

Before you begin

• The nodes must be running ONTAP 9 in a MetroCluster FC configuration. This procedure is not supported on earlier versions of ONTAP or in MetroCluster IP configurations.

• The existing MetroCluster FC configuration must be healthy.

• The equipment you are adding must be supported and meet all the requirements described in the Fabric-attached MetroCluster Installation and Configuration Guide.

• You must have available FC switch ports to accommodate the new controllers and any new bridges.

• You need the admin password and access to an FTP or SCP server.

About this task

• This procedure applies only to MetroCluster FC configurations.

• This procedure is nondisruptive and takes approximately one day to complete (excluding rack and stack) when disks are zeroed.

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

![Diagram of MetroCluster FC configuration](image)

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

**Steps**

1. **Determining the new cabling layout** on page 179
2. **Racking the new equipment** on page 179
3. **Verifying the health of the MetroCluster configuration** on page 179
4. **Checking for MetroCluster configuration errors with Config Advisor** on page 181
5. **Sending a custom AutoSupport message prior to adding nodes to the MetroCluster configuration** on page 181
6. **Recabling and zoning a switch fabric for the new nodes** on page 182
7. **Configuring ONTAP on the new controllers** on page 183
8. **Checking for MetroCluster configuration errors with Config Advisor** on page 203
9. **Sending a custom AutoSupport message after adding nodes to the MetroCluster configuration** on page 203
10. **Verifying switchover, healing, and switchback** on page 203
Determining the new cabling layout

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

About this task

This task must be performed at each MetroCluster site.

Step

1. Use the Fabric-attached MetroCluster Installation and Configuration Guide and create a cabling layout for your switch type, using the port usage for an eight-node MetroCluster configuration.

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

   Fabric-attached MetroCluster installation and configuration

   Note: If your environment cannot be cabled in such a way that RCF files can be used, you must manually configure the system according to instructions found in the Fabric-attached MetroCluster Installation and Configuration Guide. Do not use this procedure if the cabling cannot use RCF files.

Racking the new equipment

You must rack the equipment for the new nodes.

Step

1. Use the MetroCluster Installation and Configuration guide and rack the new storage systems, disk shelves, and FC-to-SAS bridges.

   Fabric-attached MetroCluster installation and configuration

Verifying the health of the MetroCluster configuration

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

Steps

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

   metrocluster show

   Example

   ```
   cluster_A::> metrocluster show
   Cluster ------------ Entry Name       State
   Local: cluster_A Configuration state configured
         Mode          normal
         AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B Configuration state configured
           Mode          normal
           AUSO Failure Domain auso-on-cluster-disaster
   ```
2. Check that mirroring is enabled on each node:
   `metrocluster node show`

   **Example**

   ```
   cluster_A::> metrocluster node show
   
   DR          Configuration        DR
   Group       Cluster     Node           State          Mirroring Mode
   ----        ------       -------           ------          ---------          -------------------
   1           cluster_A   node_A_1       configured     enabled   normal
   node_A_2       configured     enabled   normal
   cluster_B   node_B_1       configured     enabled   normal
   node_B_2       configured     enabled   normal
   4 entries were displayed.
   ```

3. Check that the MetroCluster components are healthy:
   `metrocluster check run`

   **Example**

   ```
   cluster_A::> metrocluster check run
   
   Last Checked On: 10/1/2014 16:03:37
   
   Component           Result
   ------------------- ---------
   nodes               ok
   lifs                ok
   config-replication  ok
   aggregates          ok
   4 entries were displayed.
   
   Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

   To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.
   ```

4. Check that there are no health alerts:
   `system health alert show`

5. Simulate a switchover operation:
   a. From any node's prompt, change to the advanced privilege level:
      ```
      set -privilege advanced
      
      You need to respond with y when prompted to continue into advanced mode and see the advanced mode prompt (*>).
      ```
   b. Perform the switchover operation with the -simulate parameter:
      ```
      metrocluster switchover -simulate
      ```
   c. Return to the admin privilege level:
      ```
      set -privilege admin
      ```
Checking for MetroCluster configuration errors with Config Advisor

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

About this task

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

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

Steps

1. Go to the Config Advisor download page and download the tool.
   
   NetApp Downloads: Config Advisor

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

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

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

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.

2. Invoke an AutoSupport message indicating the start of the maintenance:

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

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

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

3. Repeat this step on the partner site.
Recabling and zoning a switch fabric for the new nodes

When adding nodes to the MetroCluster configuration, you must change the cabling and then run RCF files to redefine the zoning on the fabric.

About this task
This task must be performed on each switch fabric. It is done one fabric at a time.

Disconnecting the existing DR group from the fabric

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

About this task
This task must be performed at each MetroCluster site.

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

   \textit{storage port disable -node node-name -port port-number}

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

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

Applying the RCF files and recabling the switches

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

Steps
1. Locate the RCF files for your configuration.

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

   \textit{NetApp Downloads: MetroCluster Configuration Files for Brocade Switches}

   \textit{NetApp Downloads: MetroCluster Configuration Files for Cisco Switches}

2. Apply the RCF files, following the directions on the download page, adjusting the ISL settings as needed.

3. Ensure that the switch configuration is saved.

4. Reboot the FC switches.

5. Cable both the pre-existing and the new FC-to-SAS bridges to the FC switches, using the cabling layout you created previously.

   The FC switch port usage must match the MetroCluster eight-node usage described in the \textit{Fabric-attached MetroCluster Installation and Configuration Guide} so that the Reference Configuration Files (RCFs) can be used.

   \textit{Fabric-attached MetroCluster installation and configuration}

   \textbf{Note:} If your environment cannot be cabled in such a way that RCF files can be used then contact technical support. Do NOT use this procedure if the cabling cannot use RCF files.
6. Verify that the ports are online by using the correct command for your switch.

<table>
<thead>
<tr>
<th>Switch vendor</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade</td>
<td>switchshow</td>
</tr>
<tr>
<td>Cisco</td>
<td>show interface brief</td>
</tr>
</tbody>
</table>

7. Cable the FC-VI ports from the existing and new controllers, using the cabling layout you created previously.

*Fabric-attached MetroCluster installation and configuration*

The FC switch port usage must match the MetroCluster eight-node usage described in the *Fabric-attached MetroCluster Installation and Configuration Guide* so that the Reference Configuration Files (RCFs) can be used.

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

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

   ```
   metrocluster interconnect adapter show
   metrocluster interconnect mirror show
   ```

9. Cable the HBA ports from the current and the new controllers.

10. On the existing controller modules, e-enable the ports connected to the switch fabric undergoing maintenance:

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

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

    ```
    boot_ontap maint
    ```

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

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

13. Return to the beginning of this process to recable the second switch fabric.

**Configuring ONTAP on the new controllers**

You must set up ONTAP on each new controller in the MetroCluster configuration, and then re-create the MetroCluster relationship between the two sites.

**Steps**

1. Restoring system defaults and configuring the HBA type on a previously used controller module on page 184
2. Assigning disk ownership in AFF systems on page 185
3. Assigning disk ownership in non-AFF systems on page 187
4. Verifying the ha-config state of components on page 189
5. Booting the new controllers and joining them to the cluster on page 189
6. Configuring the clusters into a MetroCluster configuration on page 191
Restoring system defaults and configuring the HBA type on a previously used controller module

If your controller modules have been used previously, you must reset them for a successful MetroCluster configuration.

About this task

**Important:** This task is required only on controller modules that have been previously configured. You do not need to perform this task if you received the controller modules from the factory.

Steps

1. At the LOADER prompt, return the environmental variables to their default setting:
   ```
   set-defaults
   ```

2. Boot the node into Maintenance mode, and then configure the settings for any HBAs in the system:
   - If you have this type of HBA and desired mode...
     - Use this command...
     - CNA FC:
       ```
       ucadmin modify -m fc -t initiator adapter_name
       ```
     - CNA Ethernet:
       ```
       ucadmin modify -mode cna adapter_name
       ```
     - FC target:
       ```
       fcadmin config -t target adapter_name
       ```
     - FC initiator:
       ```
       fcadmin config -t initiator adapter_name
       ```

3. Exit Maintenance mode:
   ```
   halt
   ```
   After you run the command, wait until the node stops at the LOADER prompt.

4. Boot the node back into Maintenance mode to enable the configuration changes to take effect.

5. Verify the changes you made:
   - If you have this type of HBA...
     - Use this command...
     - CNA:
       ```
       ucadmin show
       ```
     - FC:
       ```
       fcadmin show
       ```

6. Exit Maintenance mode:
   ```
   halt
   ```
   After you run the command, wait until the node stops at the LOADER prompt.

7. Boot the node to the boot menu:
   ```
   boot_ontap menu
   ```
   After you run the command, wait until the boot menu is shown.

8. Clear the node configuration by typing `wipeconfig` at the boot menu prompt, and then press Enter.
   The following screen shows the boot menu prompt:

   Please choose one of the following:
Assigning disk ownership in AFF systems

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

Before you begin

The storage controllers must be in Maintenance mode.

About this task

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

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

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

Steps

1. If you have not done so, boot each system into Maintenance mode.

2. Assign the disks to the nodes located at the first site (site A):
   
   You should assign an equal number of disks to each pool.
   
   a. On the first node, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:

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

   **Example**

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

   ```
   *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
   *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4
   *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
   *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
   ```
b. Repeat the process for the second node at the local site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:

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

**Example**

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

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

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

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

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

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

**Example**

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

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

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

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

**Example**

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

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirm the disk assignments:

```
storage show disk
```

5. Exit Maintenance mode:

```
halt
```

6. Display the boot menu:

```
boot_ontap menu
```

7. On each node, select option 4 to initialize all disks.
Assigning disk ownership in non-AFF systems

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

Before you begin
The storage controllers must be in Maintenance mode.

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

Note: Pool 0 always contains the disks that are found at the same site as the storage system that owns them.

Pool 1 always contains the disks that are remote to the storage system that owns them.

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

<table>
<thead>
<tr>
<th>Assign these disks in the drawer...</th>
<th>To this node and pool...</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 2</td>
<td>Local node's pool 0</td>
</tr>
<tr>
<td>3 - 5</td>
<td>HA partner node's pool 0</td>
</tr>
<tr>
<td>6 - 8</td>
<td>DR partner of the local node's pool 1</td>
</tr>
<tr>
<td>9 - 11</td>
<td>DR partner of the HA partner's pool 1</td>
</tr>
</tbody>
</table>

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

Steps
1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disk shelves to the nodes located at the first site (site A):
   Disk shelves at the same site as the node are assigned to pool 0 and disk shelves located at the partner site are assigned to pool 1.
   You should assign an equal number of shelves to each pool.
   a. On the first node, systematically assign the local disk shelves to pool 0 and the remote disk shelves to pool 1:

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

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

   ```
   *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
   *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0
   *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
   *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
   ```
b. Repeat the process for the second node at the local site, systematically assigning the local disk shelves to pool 0 and the remote disk shelves to pool 1:

\[
\text{disk assign -shelf local-switch-name:shelf-name.port -p pool}
\]

**Example**

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

\[
\text{\*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0}
\]

\[
\text{\*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1}
\]

\[
\text{\*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0}
\]

\[
\text{\*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1}
\]

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

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

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

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

   \[
   \text{disk assign -shelf local-switch-name:shelf-name -p pool}
   \]

   **Example**

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

   \[
   \text{\*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0}
   \]

   \[
   \text{\*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0}
   \]

   \[
   \text{\*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1}
   \]

   \[
   \text{\*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1}
   \]

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

   \[
   \text{disk assign -shelf shelf-name -p pool}
   \]

   **Example**

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

   \[
   \text{\*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0}
   \]

   \[
   \text{\*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0}
   \]

   \[
   \text{\*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1}
   \]

   \[
   \text{\*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1}
   \]

4. Confirm the shelf assignments:

   \[
   \text{storage show shelf}
   \]

5. Exit Maintenance mode:

   \[
   \text{halt}
   \]

6. Display the boot menu:

   \[
   \text{boot_ontap menu}
   \]

7. On each node, select option 4 to initialize all disks.
Verifying the ha-config state of components

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

Before you begin
The system must be in Maintenance mode.

About this task
This task must be performed on each new controller module.

Steps
1. In Maintenance mode, display the HA state of the controller module and chassis:
   
   `ha-config show`

   The HA state for all components should be mcc.

2. If the displayed system state of the controller is not correct, set the HA state for the controller module:
   
   `ha-config modify controller mcc`

3. If the displayed system state of the chassis is not correct, set the HA state for the chassis:
   
   `ha-config modify chassis mcc`

4. Repeat these steps on the other replacement node.

Booting the new controllers and joining them to the cluster

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

Before you begin
You must have cabled the MetroCluster configuration.

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

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

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

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

   `boot_ontap`

   The controller module enters the node setup wizard.

Example
The output should be similar to the following:
Welcome to node setup

You can enter the following commands at any time:
"help" or ":?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the setup wizard.

Any changes you made before quitting will be saved.

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

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

Example
The prompts are similar to the following:

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

4. Confirm that nodes are configured in high-availability mode:
   
   **storage failover show -fields mode**

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

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

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

5. Confirm that you have four ports configured as cluster interconnects:
   
   **network port show**

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

   **cluster_A::> network port show**

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>ISpace</th>
<th>Broadcast</th>
<th>Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Speed (Mbps)</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td></td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0a</td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0e</td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0g</td>
<td></td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>node_A_2</td>
<td></td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0a</td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0e</td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e0g</td>
<td></td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

   exit

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

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

   cluster setup

   ::> cluster setup

   Welcome to the cluster setup wizard.

   You can enter the following commands at any time:
   "help" or "?" - if you want to have a question clarified,
   "back" - if you want to change previously answered questions, and
   "exit" or "quit" - if you want to quit the cluster setup wizard.
   Any changes you made before quitting will be saved.

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

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

   join

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

   cluster show

   Example

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

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

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

   Configuring the clusters into a MetroCluster configuration

   You must peer the clusters, mirror the root aggregates, create a mirrored data aggregate, and then issue the command to implement the MetroCluster operations.

   Steps
   1. Configuring intercluster LIFs on page 192
   2. Mirroring the root aggregates on page 195
   3. Implementing the MetroCluster configuration on page 196
   4. Creating a mirrored data aggregate on each node on page 197
   5. Creating unmirrored data aggregates on page 199
   6. Configuring FC-to-SAS bridges for health monitoring on page 200
   7. Checking the MetroCluster configuration on page 201
Configuring intercluster LIFs

You must create intercluster LIFs on ports used for communication between the MetroCluster partner clusters. You can use dedicated ports or ports that also have data traffic.

Choices
- Configuring intercluster LIFs on dedicated ports on page 192
- Configuring intercluster LIFs on shared data ports on page 194

Configuring intercluster LIFs on dedicated ports

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

Steps

1. List the ports in the cluster:
   
   network port show
   
   For complete command syntax, see the man page.

   Example
   
   The following example shows the network ports in cluster01:

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster01-01</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>cluster01-02</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
</tbody>
</table>

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

   network interface show -fields home-port,curr-port
   
   For complete command syntax, see the man page.

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

<table>
<thead>
<tr>
<th>vserver lif</th>
<th>home-port</th>
<th>curr-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>e0a</td>
<td>e0a</td>
</tr>
<tr>
<td>Cluster</td>
<td>e0b</td>
<td>e0b</td>
</tr>
<tr>
<td>Cluster</td>
<td>e0a</td>
<td>e0a</td>
</tr>
<tr>
<td>Cluster</td>
<td>e0b</td>
<td>e0b</td>
</tr>
<tr>
<td>Cluster</td>
<td>e0c</td>
<td>e0c</td>
</tr>
<tr>
<td>Cluster</td>
<td>e0c</td>
<td>e0c</td>
</tr>
<tr>
<td>Cluster</td>
<td>e0c</td>
<td>e0c</td>
</tr>
</tbody>
</table>

network port show

For complete command syntax, see the man page.
3. Create a failover group for the dedicated ports:

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

**Example**

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

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

4. Verify that the failover group was created:

```
network interface failover-groups show
```

For complete command syntax, see the man page.

**Example**

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

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

```
network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group
```

For complete command syntax, see the man page.

**Example**

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

```
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01 -role intercluster -home-node cluster01-01 -home-port e0e -address 192.168.1.201 -netmask 255.255.255.0 -failover-group intercluster01
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl02 -role intercluster -home-node cluster01-02 -home-port e0e -address 192.168.1.202 -netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

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

For complete command syntax, see the man page.

**Example**

```
cluster01::> network interface show -role intercluster
               Logical       Network   Current       Current Is
               Vserver       Interface Admin/Oper Address/Mask       Node     Port     Home
               --------------- ------------- ------------- ------------------ ------- ------- ----
```
7. Verify that the intercluster LIFs are redundant:

   network interface show -role intercluster -failover

For complete command syntax, see the man page.

Example

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

```
cluster01::> network interface show -role intercluster -failover
```

<table>
<thead>
<tr>
<th>Logical Vserver</th>
<th>Interface</th>
<th>Home:Port</th>
<th>Failover Policy</th>
<th>Failover Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster01-01</td>
<td>cluster01-01_icl01</td>
<td>cluster01-01:e0e</td>
<td>local-only</td>
<td>intercluster01, cluster01-01:e0e, cluster01-01:e0f</td>
</tr>
<tr>
<td>cluster01-01</td>
<td>cluster01-01_icl02</td>
<td>cluster01-02:e0e</td>
<td>local-only</td>
<td>intercluster01, cluster01-02:e0e, cluster01-02:e0f</td>
</tr>
</tbody>
</table>

Configuring intercluster LIFs on shared data ports

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

Steps

1. List the ports in the cluster:

   network port show

   For complete command syntax, see the man page.

Example

The following example shows the network ports in `cluster01`:

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Speed (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
</tbody>
</table>

2. Create intercluster LIFs on the system SVM:

   network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask

   For complete command syntax, see the man page.

Example

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02`:
3. Verify that the intercluster LIFs were created:

   network interface show -role intercluster

For complete command syntax, see the man page.

Example

```
cluster01::> network interface show -role intercluster
Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01  cluster01_icl01 up/up   192.168.1.201/24   cluster01-01  e0c     true
cluster01  cluster01_icl02 up/up   192.168.1.202/24   cluster01-02  e0c     true
```

4. Verify that the intercluster LIFs are redundant:

   network interface show -role intercluster -failover

For complete command syntax, see the man page.

Example

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

```
cluster01::> network interface show -role intercluster -failover
Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01  cluster01_icl01 cluster01-01:e0c   local-only      192.168.1.201/24
cluster01  cluster01_icl02 cluster01-01:e0d   local-only      192.168.1.201/24
cluster01  cluster01_icl01 cluster01-02:e0c   local-only      192.168.1.201/24
cluster01  cluster01_icl02 cluster01-02:e0d   local-only      192.168.1.201/24
```

### Mirroring the root aggregates

You must mirror the root aggregates to provide data protection.

**About this task**

By default, the root aggregate is created as RAID-DP type aggregate. You can change the root aggregate from RAID-DP to RAID4 type aggregate. The following command modifies the root aggregate for RAID4 type aggregate:

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```

**Note:** On non-ADP systems, the RAID type of the aggregate can be modified from the default RAID-DP to RAID4 before or after the aggregate is mirrored.

**Steps**

1. Mirror the root aggregate:
storage aggregate mirror aggr_name

Example

The following command mirrors the root aggregate for controller_A_1:

controller_A_1::> storage aggregate mirror aggr0_controller_A_1

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

2. Repeat the previous step for each node in the MetroCluster configuration.

Implementing the MetroCluster configuration

You must run the `metrocluster configure -refresh true` command to start data protection on the nodes that you have added to a MetroCluster configuration.

Before you begin

- The ha-config state of the controllers and chassis must be `mcc`.

About this task

You issue the `metrocluster configure -refresh true` command once, on one of the newly added nodes, to refresh the MetroCluster configuration. You do not need to issue the command on each of the sites or nodes.

The `metrocluster configure -refresh true` command automatically pairs the two nodes with the lowest system IDs in each of the two clusters as disaster recovery (DR) partners. In a four-node MetroCluster configuration, there are two DR partner pairs. The second DR pair is created from the two nodes with higher system IDs.

Steps

1. Refresh the MetroCluster configuration:
   
   a. Enter advanced privilege mode:
      
      ```
      set -privilege advanced
      ```
   
   b. Refresh the MetroCluster configuration on one of the new nodes:
      
      ```
      metrocluster configure -refresh true
      ```
   
   Example

   The following example shows the MetroCluster configuration refreshed on both DR groups:

   ```
   controller_A_2::*> metrocluster configure -refresh true
   [Job 726] Job succeeded: Configure is successful.
   
   controller_A_4::*> metrocluster configure -refresh true
   [Job 740] Job succeeded: Configure is successful.
   ```

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

2. Verify the networking status on site A:

   ```
   network port show
   ```
### Example

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

```plaintext
cluster_A1::> network port show

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPSpace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster_A_1</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
</tbody>
</table>

controller_A_2

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPSpace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
</tbody>
</table>

14 entries were displayed.
```

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

a. Verify the configuration from site A:

```
metrocluster show
```

#### Example

```plaintext
cluster_A1::> metrocluster show

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Entry Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local:</td>
<td>cluster_A</td>
<td>Configuration state configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode: normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AUSO Failure Domain: auso-on-cluster-disaster</td>
</tr>
<tr>
<td>Remote:</td>
<td>cluster_B</td>
<td>Configuration state configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode: normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AUSO Failure Domain: auso-on-cluster-disaster</td>
</tr>
</tbody>
</table>
```

b. Verify the configuration from site B:

```
metrocluster show
```

#### Example

```plaintext
cluster_B::> metrocluster show

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Entry Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local:</td>
<td>cluster_B</td>
<td>Configuration state configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode: normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AUSO Failure Domain: auso-on-cluster-disaster</td>
</tr>
<tr>
<td>Remote:</td>
<td>cluster_A</td>
<td>Configuration state configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode: normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AUSO Failure Domain: auso-on-cluster-disaster</td>
</tr>
</tbody>
</table>
```

### Creating a mirrored data aggregate on each node

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

#### Before you begin

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

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

Disk and aggregate management

Steps

1. Display a list of available spares:

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

2. Create the aggregate by using the `storage aggregate create -mirror true` command.

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

   You can specify the following options:
   - Aggregate's home node (that is, the node that owns the aggregate in normal operation)
   - List of specific drives or array LUNs that are to be added to the aggregate
   - Number of drives to include

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

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

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

Example

The following command creates a mirrored aggregate with 10 disks:

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

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

   ```sh
   storage aggregate show-status -aggregate aggregate-name
   ```
Creating unmirrored data aggregates

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

Before you begin

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

About this task

Attention:

In MetroCluster FC configurations, the unmirrored aggregates will only be online after a switchover if the remote disks in the aggregate are accessible. If the ISLs fail, the local node may be unable to access the data in the unmirrored remote disks. The failure of an aggregate can lead to a reboot of the local node.

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

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

Steps

1. Display a list of available spares:

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

2. Create the aggregate:

   ```
   storage aggregate create
   ```

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

   You can specify the following options:

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

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

**Example**

The following command creates a unmirrored aggregate with 10 disks:

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

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

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

**Related information**

*Disk and aggregate management*

**Configuring FC-to-SAS bridges for health monitoring**

You must perform some special configuration steps to monitor the FC-to-SAS bridges in the MetroCluster configuration.

**About this task**

Third-party SNMP monitoring tools are not supported for FibreBridge bridges.

**Step**

1. From the ONTAP cluster prompt, add the bridge to health monitoring:
   a. Add the bridge, using the command for your version of ONTAP:

   ```
<table>
<thead>
<tr>
<th>ONTAP version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 and later</td>
<td><code>storage bridge add -address 0.0.0.0 -managed-by in-band -name bridge-name</code></td>
</tr>
<tr>
<td>9.4 and earlier</td>
<td><code>storage bridge add -address bridge-ip-address -name bridge-name</code></td>
</tr>
</tbody>
</table>
   ```
   b. Verify that the bridge has been added and is properly configured:
      ```
      storage bridge show
      ```
      It might take as long as 15 minutes to reflect all data because of the polling interval. The ONTAP health monitor can contact and monitor the bridge if the value in the Status column is `ok`, and other information, such as the worldwide name (WWN), is displayed.

   **Example**

   The following example shows that the FC-to-SAS bridges are configured:

   ```bash
   controller_A_1::> storage bridge show
   Bridge Model    Symbolic Name Is Monitored        Monitor Status  Vendor
   ----------------- --------------- ------------- -------------- -------
   ----------------- --------------- ------------- -------------- -------
   ```
Checking the MetroCluster configuration

You can check that the components and relationships in the MetroCluster configuration are working correctly. You should do a check after initial configuration and after making any changes to the MetroCluster configuration. You should also do a check before a negotiated (planned) switchover or a switchback operation.

About this task

If the `metrocluster check run` command is issued twice within a short time on either or both clusters, a conflict can occur and the command might not collect all data. Subsequent `metrocluster check show` commands do not show the expected output.

Steps

1. Check the configuration:

   `metrocluster check run`

   Example

   The command runs as a background job and might not be completed immediately.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait for it to complete and run "metrocluster check show" to view the results. To check the status of the running metrocluster check operation, use the command, "metrocluster operation history show -job-id 2245"
   ```

   ```
   cluster_A::> metrocluster check show
   Last Checked On: 9/13/2017 20:41:37
   Component           Result
   ------------------- ---------
   nodes               ok
   lifs                ok
   config-replication  ok
   aggregates          ok
   clusters            ok
   5 entries were displayed.
   ```

2. Display more detailed results from the most recent `metrocluster check run` command:

   `metrocluster check aggregate show`

   `metrocluster check cluster show`

   `metrocluster check config-replication show`

   `metrocluster check lif show`
**metrocluster check node show**

The `metrocluster check show` commands show the results of the most recent `metrocluster check run` command. You should always run the `metrocluster check run` command prior to using the `metrocluster check show` commands so that the information displayed is current.

**Example**

The following example shows the `metrocluster check aggregate show` command output for a healthy four-node MetroCluster configuration:

```
cluster_A::> metrocluster check aggregate show
Last Checked On: 8/5/2014 00:42:58

<table>
<thead>
<tr>
<th>Node</th>
<th>Aggregate</th>
<th>Check</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_A_1</td>
<td>controller_A_1_aggr0</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_1</td>
<td>controller_A_1_aggr1</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_1</td>
<td>controller_A_1_aggr2</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_2</td>
<td>controller_A_2_aggr0</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_2</td>
<td>controller_A_2_aggr1</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_2</td>
<td>controller_A_2_aggr2</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
</tbody>
</table>

18 entries were displayed.
```

The following example shows the `metrocluster check cluster show` command output for a healthy four-node MetroCluster configuration. It indicates that the clusters are ready to perform a negotiated switchover if necessary.

```
Last Checked On: 9/13/2017 20:47:04

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Check</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>mccint-fas9000-0102</td>
<td>negotiated-switchover-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>switchback-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>job-schedules</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>licenses</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>periodic-check-enabled</td>
<td>ok</td>
</tr>
<tr>
<td>mccint-fas9000-0304</td>
<td>negotiated-switchover-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>switchback-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>job-schedules</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>licenses</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>periodic-check-enabled</td>
<td>ok</td>
</tr>
</tbody>
</table>

10 entries were displayed.
```
Checking for MetroCluster configuration errors with Config Advisor

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

About this task

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

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

Steps

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

   NetApp Downloads: Config Advisor

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

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

You should issue an AutoSupport message to notify NetApp technical support that maintenance is complete.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.

2. Invoke an AutoSupport message indicating the end of the maintenance:

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

3. Repeat this step on the partner site.

Verifying switchover, healing, and switchback

You should verify the switchover, healing, and switchback operations of the MetroCluster configuration.

Step

1. Use the procedures for negotiated switchover, healing, and switchback that are mentioned in the MetroCluster Management and Disaster Recovery Guide.

   MetroCluster management and disaster recovery
Reconfiguring the FC switch layout for ONTAP 9.1 or later

If your existing FC switch layout was configured prior to ONTAP 9.1, you must reconfigure the port layout and apply the latest Reference Configuration Files (RCFs). This procedure applies only to MetroCluster FC configurations.

Before you begin
You must identify the FC switches present in the fabric domain.
You need the admin password and access to an FTP or SCP server.

About this task
You must perform this task if your existing FC switch layout was configured prior to ONTAP 9.1 and you are upgrading to a platform model supported in ONTAP 9.1 or later. It is not required if you are upgrading from an existing switch layout that was configured for ONTAP 9.1 or later.

This procedure is nondisruptive and takes approximately four hours to complete (excluding rack and stack) when disks are zeroed.

Steps
1. Sending a custom AutoSupport message prior to reconfiguring switches on page 204
2. Verifying the health of the MetroCluster configuration on page 205
3. Checking for MetroCluster configuration errors on page 206
4. Persistently disabling the switches on page 206
5. Determining the new cabling layout on page 207
6. Applying RCF files and recabling the switches on page 207
7. Persistently enable the switches on page 208
8. Verifying switchover, healing, and switchback on page 208

Sending a custom AutoSupport message prior to reconfiguring switches

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

About this task
This task must be performed on each MetroCluster site.

Steps
1. Log in to the cluster.
2. Invoke an AutoSupport message indicating the start of the maintenance:
   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```
maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

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

3. Repeat these steps on the partner site.

### Verifying the health of the MetroCluster configuration

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

**Steps**

1. Verify that the MetroCluster components are healthy:

```
metrocluster check run
```

**Example**

```
dpgqa-mcc-funct-8040-0403_siteA::*> metrocluster check run
----
```

The operation runs in the background.

2. After the `metrocluster check run` operation completes, run `metrocluster check show` to view the results.

After approximately five minutes, the following results are displayed:

```
----------
dpgqa-mcc-funct-8040-0403_siteA::*> metrocluster check show
Last Checked On: 4/7/2019 21:15:05

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

3. To check the status of the running MetroCluster check operation, use the command:

```
metrocluster operation history show -job-id 38
```

4. Verify that there are no health alerts:

```
system health alert show
```
Checking for MetroCluster configuration errors

You can use the Config Advisor tool available from the NetApp Support Site to check for common configuration errors.

About this task

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

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

Steps

1. Download the Config Advisor tool.

   Config Advisor

2. Run Config Advisor, reviewing the output and following its recommendations to address any issues.

Persistently disabling the switches

You must disable the switches in the fabric persistently so that you can modify its configuration.

About this task

You disable the switches by running the commands on the switch command line; the commands used for this are not ONTAP commands.

Step

1. Persistently disable the switch:

   • For Brocade switches, use the switchCfgPersistentDisable command.

   • For Cisco switches, use the suspend command.

Example

The following command disables a Brocade switch persistently:

    FC_switch_A_1:admin> switchCfgPersistentDisable

Example

The following command disables a Cisco switch:

    vsan [vsna #] suspend
Determining the new cabling layout

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

About this task

This task must be performed at each MetroCluster site.

Step

1. Use the Fabric-attached MetroCluster Installation and Configuration Guide to determine the cabling layout for your switch type, using the port usage for an eight-node MetroCluster configuration.

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

Fabric-attached MetroCluster installation and configuration

   Note: If your environment cannot be cabled in a way that RCFs can be used, then contact technical support. Do not use this procedure if the cabling cannot use RCFs.

Applying RCF files and recabling the switches

You must apply the appropriate reference configuration (RCF) files to reconfigure your switches to accommodate the new nodes. After you apply the RCF files, you can recable the switches.

Before you begin

The FC switch port usage must match the usage described in the Fabric-attached MetroCluster Installation and Configuration Guide so that the RCFs can be used.

Fabric-attached MetroCluster installation and configuration

Steps

1. Locate the RCF files for your configuration.

   You must use the RCF files that match your switch model.

   NetApp Downloads: MetroCluster Configuration Files for Brocade Switches
   NetApp Downloads: MetroCluster Configuration Files for Cisco Switches

2. Apply the RCF files, following the directions on the Download page and adjusting the ISL settings as needed.

3. Verify that the switch configuration is saved.

4. Cable both of the FC-to-SAS bridges to the FC switches, using the cabling layout you created in the “Determining the new cabling layout” section.

5. Verify that the ports are online:

   • For Brocade switches, use the switchshow command.
   • For Cisco switches, use the show interface brief command.

6. Cable the FC-VI ports from the controllers to the switches.
7. From the existing nodes, verify that the FC-VI ports are online:
   ```
   metrocluster interconnect adapter show
   metrocluster interconnect mirror show
   ```

**Persistently enable the switches**

You must enable the switches in the fabric persistently.

**Step**

1. Persistently enable the switch:
   - For Brocade switches, use the `switchCfgPersistentenable` command.
   - For Cisco switches, use the `no suspend` command.

**Example**

The following command persistently enables a Brocade switch:

```
FC_switch_A_1:admin> switchCfgPersistentenable
```

**Example**

The following command enables a Cisco switch:

```
vsan [vsna #]no suspend
```

**Verifying switchover, healing, and switchback**

You should verify the switchover, healing, and switchback operations of the MetroCluster configuration.

**Step**

1. Use the procedures for negotiated switchover, healing, and switchback that are mentioned in the *MetroCluster Management and Disaster Recovery Guide*.

   *MetroCluster management and disaster recovery*
Port assignments for FC switches

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later versions of ONTAP.

Port assignments for systems using two initiator ports

You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems using a single initiator port for each fabric and two initiator ports for each controller.

You can follow the cabling for the FibreBridge 6500N bridge or FibreBridge 7500N or 7600N bridge using only one FC port (FC1 or FC2). Instead of using four initiators, connect only two initiators and leave the other two that are connected to the switch port empty.

You must apply the correct RCF file for the FibreBridge 6500N bridge's configuration.

If zoning is performed manually, then follow the zoning used for a FibreBridge 6500N or a FibreBridge 7500N or 7600N bridge using one FC port (FC1 or FC2). In this scenario, one initiator port rather than two is added to each zone member per fabric.

You can change the zoning or perform an upgrade from a FibreBridge 6500 to a FibreBridge 7500 using the procedure Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7500N or 7600N bridge from the MetroCluster Service and Expansion Guide.

The following table shows port assignments for FC switches when using ONTAP 9.1 and later.

<table>
<thead>
<tr>
<th>Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MetroCluster 1 or DR Group 1</strong></td>
</tr>
<tr>
<td>Component</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>controller_x_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Stack 1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Stack y</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The following table shows port assignments for FC switches when using ONTAP 9.0.
### Port assignments for FC switches when using ONTAP 9.0

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later versions of ONTAP.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCF files are used, ISL ports may not connect to the same ports shown here and may need to be reconfigured manually.

### Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.
  - On Cisco switches, the first port is numbered 1.
- The cabling is the same for each FC switch in the switch fabric.
- AFF A300 and FAS8200 storage systems can be ordered with one of two options for FC-VI connectivity:
  - Onboard ports 0e and 0f configured in FC-VI mode.
  - Ports 1a and 1b on an FC-VI card in slot 1.

### Brocade port usage for controller connections in an eight-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Brocade switches:
### MetroCluster eight-node configuration

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade 6505, 6510, or DCX 8510-8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC_switch_x_1</td>
<td>FC_switch_x_2</td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
</tbody>
</table>

**Brocade port usage for FC-to-SAS bridge connections in an eight-node MetroCluster configuration running ONTAP 9.0**

The following table shows bridge port usage when using FibreBridge 7500 bridges:

<table>
<thead>
<tr>
<th>FC_switch_x_1</th>
<th>FC_switch_x_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
</tr>
</tbody>
</table>
The following table shows bridge port usage when using FibreBridge 6500 bridges:

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge</th>
<th>Port</th>
<th>Brocade 6505, 6510, or DCX 8510-8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>16</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>17</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>18</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>19</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
</tr>
</tbody>
</table>

Brocade port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>ISL port</th>
<th>Brocade 6505, 6510, or DCX 8510-8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>ISL port 1</td>
<td>20</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>21</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>22</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>23</td>
</tr>
</tbody>
</table>
Brocade port usage for controllers in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

| MetroCluster four-node configuration | Port | | | Brocade 6505, 6510, or DCX 8510-8 | | | | FC_switch_x_1 | FC_switch_x_2 |
| Component | Port | | | | | | | | | |
| controller_x_1 | FC-VI port a | 0 | | - | | | | | |
| | FC-VI port b | - | | 0 | | | | | |
| | HBA port a | 1 | | - | | | | | |
| | HBA port b | - | | 1 | | | | | |
| | HBA port c | 2 | | - | | | | | |
| | HBA port d | - | | 2 | | | | | |
| controller_x_2 | FC-VI port a | 3 | | - | | | | | |
| | FC-VI port b | - | | 3 | | | | | |
| | HBA port a | 4 | | - | | | | | |
| | HBA port b | - | | 4 | | | | | |
| | HBA port c | 5 | | - | | | | | |
| | HBA port d | - | | 5 | | | | | |

Brocade port usage for bridges in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges. Additional bridges can be cabled to ports 18 through 23.

| MetroCluster four-node configuration | Port | | | Brocade 6510 or DCX 8510-8 | | | | Brocade 6505 | | | | FC_switch_x_1 | FC_switch_x_2 | FC_switch_x_1 | FC_switch_x_2 |
| FibreBridge 7500 bridge | Port | | | | | | | | | | | | | | | | | |
| bridge_x_1a | FC1 | 6 | | - | | 6 | | - | | | | | | | | | | | |
| | FC2 | - | | 6 | | - | | 6 | | | | | | | | | | | |
| bridge_x_1b | FC1 | 7 | | - | | 7 | | - | | | | | | | | | | | |
| | FC2 | - | | 7 | | - | | 7 | | | | | | | | | | | |
| bridge_x_2a | FC1 | 8 | | - | | 12 | | - | | | | | | | | | | | |
| | FC2 | - | | 8 | | - | | 12 | | | | | | | | | | | |
| bridge_x_2b | FC1 | 9 | | - | | 13 | | - | | | | | | | | | | | |
| | FC2 | - | | 9 | | - | | 13 | | | | | | | | | | | |
| bridge_x_3a | FC1 | 10 | | - | | 14 | | - | | | | | | | | | | | |
| | FC2 | - | | 10 | | - | | 14 | | | | | | | | | | | |
### MetroCluster four-node configuration

<table>
<thead>
<tr>
<th>FibreBridge 7500 bridge</th>
<th>Port</th>
<th>Brocade 6510 or DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
<td>FC_switch_x_2</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>13</td>
</tr>
</tbody>
</table>

Additional bridges can be cabled through port 19, then ports 24 through 47

Additional bridges can be cabled through port 23

### The following table shows bridge port usage when using FibreBridge 6500 bridges:

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge</th>
<th>Port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
<td>FC_switch_x_2</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
<td>8</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
<td>13</td>
</tr>
</tbody>
</table>

Additional bridges can be cabled through port 19, then ports 24 through 47

Additional bridges can be cabled through port 23
Brocade port usage for ISLs in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>MetroCluster four-node configuration</th>
<th>ISL port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISL port 1</td>
<td>FC_switch_x_1</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>FC_switch_x_2</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>FC_switch_x_1</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>FC_switch_x_2</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

Brocade port usage for controllers in a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

<table>
<thead>
<tr>
<th>MetroCluster two-node configuration</th>
<th>Component</th>
<th>Port</th>
<th>Brocade 6505, 6510, or DCX 8510-8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port c</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port d</td>
<td>-</td>
</tr>
</tbody>
</table>

Brocade port usage for bridges in a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges. Additional bridges can be cabled to ports 18 through 23.

<table>
<thead>
<tr>
<th>MetroCluster two-node configuration</th>
<th>FibreBridge 7500 bridge</th>
<th>Port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1a</td>
<td>FC2</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1b</td>
<td>FC2</td>
<td>-</td>
<td>7</td>
</tr>
</tbody>
</table>
The following table shows bridge port usage when using FibreBridge 7500 bridges:

<table>
<thead>
<tr>
<th>FibreBridge 7500 bridge</th>
<th>Port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC1</td>
<td>FC2</td>
<td>FC1</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>8</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>-</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>9</td>
<td>-</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>-</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>10</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>-</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>11</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>-</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>12</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>-</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>13</td>
<td>-</td>
<td>17</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>-</td>
<td>13</td>
<td>-</td>
</tr>
</tbody>
</table>

Additional bridges can be cabled through port 19, then ports 24 through 47.

The following table shows bridge port usage when using FibreBridge 6500 bridges:

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge</th>
<th>Port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC1</td>
<td>FC2</td>
<td>FC1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>6</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>-</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>7</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>-</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>8</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>-</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>9</td>
<td>-</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>-</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>10</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>-</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>11</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>-</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>12</td>
<td>-</td>
<td>16</td>
</tr>
</tbody>
</table>
MetroCluster two-node configuration

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge</th>
<th>Port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
<td>FC_switch_x_2</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
<td>13</td>
</tr>
</tbody>
</table>

Additional bridges can be cabled through port 19, then ports 24 through 47.

Brocade port usage for ISLs in a two-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>ISL port</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC_switch_x_1</td>
<td>FC_switch_x_2</td>
</tr>
<tr>
<td>ISL port 1</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>23</td>
<td>23</td>
</tr>
</tbody>
</table>

Cisco port usage for controllers in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows controller port usage on Cisco switches:

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
</tbody>
</table>
### MetroCluster eight-node configuration

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
</tbody>
</table>

**Cisco port usage for FC-to-SAS bridges in an eight-node MetroCluster configuration running ONTAP 9.0**

The following table shows bridge port usage up to port 23 when using FibreBridge 7500 bridges. Additional bridges can be attached using ports 25 through 48.

<table>
<thead>
<tr>
<th>FibreBridge 7500 bridge</th>
<th>Port</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td></td>
</tr>
</tbody>
</table>

Additional bridges can be attached using ports 25 through 48 following the same pattern.
FibreBridge 6500 bridge  | Port | Cisco 9148 or 9148S
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>17</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>18</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>19</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>21</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>22</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>23</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
</tr>
</tbody>
</table>

Additional bridges can be attached using ports 25 through 48 following the same pattern.

Cisco port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>ISL port</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>ISL port 1</td>
<td>12</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>16</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>20</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>24</td>
</tr>
</tbody>
</table>

Cisco port usage for controllers in a four-node MetroCluster configuration

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco switches:
### MetroCluster four-node configuration

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Cisco 9148, 9148S, or 9250i</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
</tbody>
</table>

### Cisco port usage for FC-to-SAS bridges in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges. Additional bridges can be attached to ports 15 through 32 following the same pattern.

<table>
<thead>
<tr>
<th>FibreBridge 7500 bridge</th>
<th>Port</th>
<th>Cisco 9148, 9148S, or 9250i</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
</tbody>
</table>
The following table shows bridge port usage when using FibreBridge 6500 bridges up to port 14. Additional bridges can be attached to ports 15 through 32 following the same pattern.

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge</th>
<th>Port</th>
<th>Cisco 9148, 9148S, or 9250i</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>7</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>8</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
</tr>
</tbody>
</table>

Additional bridges can be attached to ports 15 through 32 following the same pattern.

**Cisco 9148 and 9148S port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0**

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>ISL port</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>ISL port 1</td>
<td>36</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>40</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>44</td>
</tr>
</tbody>
</table>
**MetroCluster four-node configuration**

<table>
<thead>
<tr>
<th>ISL port</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>48</td>
</tr>
</tbody>
</table>

**Cisco 9250i port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0**

The Cisco 9250i switch uses the FCIP ports for the ISL. See NetApp Knowledgebase Answer 1030474: How to configure the Cisco 9250i FC storage back end switch in MetroCluster for clustered Data ONTAP for limitations and procedures for using the FCIP ports.

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

**Cisco port usage for controllers in a two-node MetroCluster configuration**

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco switches:

<table>
<thead>
<tr>
<th>MetroCluster two-node configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
</tr>
<tr>
<td>controller_x_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Cisco port usage for FC-to-SAS bridges in a two-node MetroCluster configuration running ONTAP 9.0**

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges. Additional bridges can be attached to ports 15 through 32 following the same pattern.

<table>
<thead>
<tr>
<th>MetroCluster two-node configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreBridge 7500 bridge</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_1a</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_1b</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_2a</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The following table shows bridge port usage when using FibreBridge 6500 bridges up to port 14. Additional bridges can be attached to ports 15 through 32 following the same pattern.

### MetroCluster two-node configuration

<table>
<thead>
<tr>
<th>FibreBridge 7500 bridge</th>
<th>Port</th>
<th>Cisco 9148, 9148S, or 9250i</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
</tbody>
</table>

Additional bridges can be attached to ports 15 through 32 following the same pattern.

### MetroCluster two-node configuration

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge</th>
<th>Port</th>
<th>Cisco 9148, 9148S, or 9250i</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>7</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>8</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
</tr>
</tbody>
</table>

Additional bridges can be attached to ports 15 through 32 following the same pattern.
Cisco 9148 or 9148S port usage for ISLs on a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>MetroCluster two-node configuration</th>
<th>Cisco 9148 or 9148S</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISL port</td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>ISL port 1</td>
<td>36</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>40</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>44</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>48</td>
</tr>
</tbody>
</table>

Cisco 9250i port usage for ISLs on a two-node MetroCluster configuration running ONTAP 9.0

The Cisco 9250i switch uses the FCIP ports for the ISL. See NetApp Knowledgebase Answer 1030474: How to configure the Cisco 9250i FC storage back end switch in MetroCluster for clustered Data ONTAP for limitations and procedures for using the FCIP ports.

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

Port assignments for FC switches when using ONTAP 9.1 and later

You need to verify that you are using the specified port assignments when you cable the FC switches when using ONTAP 9.1 and later.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCFs are used, ISL ports might not connect to the same ports shown here and might need to be reconfigured manually.

If you configured your switches using the port assignments for ONTAP 9, you can continue to use the older assignments. However, new configurations running ONTAP 9.1 or later releases should use the port assignments shown here.

Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.
  - On Cisco switches, the first port is numbered 1.

- The cabling is the same for each FC switch in the switch fabric.

- AFF A300 and FAS8200 storage systems can be ordered with one of two options for FC-VI connectivity:
  - Onboard ports 0e and 0f configured in FC-VI mode.
• Ports 1a and 1b on an FC-VI card in slot 1.

• AFF A700 and FAS9000 storage systems require four FC-VI ports. The following tables show cabling for the FC switches with four FC-VI ports on each controller.

For other storage systems, use the cabling shown in the tables but ignore the cabling for FC-VI ports c and d. You can leave those ports empty.

• If you have two MetroCluster configurations sharing ISLs, use the same port assignments as that for an eight-node MetroCluster cabling. The number of ISLs you cable may vary depending on your site's requirements. See the section on ISL considerations.

Brocade port usage for controllers in a MetroCluster configuration running ONTAP 9.1 or later

The following tables show port usage on Brocade switches. The tables show the maximum supported configuration, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules. Note that eight ISLs are supported only on the Brocade 6510, Brocade DCX 8510-8, G620, and G630 switches.

Note: Port usage for the Brocade 6505 and Brocade G610 switches in an eight-node MetroCluster configuration is not shown. Due to the limited number of ports, port assignments must be made on a site-by-site basis depending on the controller module model and the number of ISLs and bridge pairs in use.

Note: The Brocade DCX 8510-8 switch can use the same port layout as the 6510 switch or the 7840 switch.

| Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only |
|---|---|---|---|
| **Component** | **Port** | **Brocade switch models 6505, 6510, 6520, 7840, G610, G620, G630, and DCX 8510-8** | **MetroCluster 1 or DR Group 1** |
| Stack 1 | bridge_x_1a | | 1 |
| | bridge_x_1b | Connects to FC switch... | 8 |
| Stack 2 | bridge_x_2a | 1 | 9 |
| | bridge_x_2b | Connects to switch port... | 9 |
| Stack 3 | bridge_x_3a | 1 | 10 |
| | bridge_x_4b | Connects to switch port... | 10 |
| Stack y | bridge_x_ya | 1 | 11 |
| | bridge_x_yb | Connects to switch port... | 11 |

Note:

• On G620 and G630 switches, additional bridges can be cabled to ports 12 - 17, 20 and 21.

• On G610 switches, additional bridges can be cabled to ports 12 - 19.
Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

MetroCluster 2 or DR Group 2

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Connects to FC_switch...</th>
<th>6510, DCX 8510-8</th>
<th>6520</th>
<th>7840, DCX 8510-8</th>
<th>G620, G630</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>1</td>
<td>24</td>
<td>48</td>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
<td>24</td>
<td>48</td>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td>25</td>
<td>49</td>
<td>13</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
<td>25</td>
<td>49</td>
<td>13</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
<td>26</td>
<td>50</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
<td>26</td>
<td>50</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
<td>27</td>
<td>51</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
<td>27</td>
<td>51</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>1</td>
<td>28</td>
<td>52</td>
<td>16</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
<td>28</td>
<td>52</td>
<td>16</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td>29</td>
<td>53</td>
<td>17</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
<td>29</td>
<td>53</td>
<td>17</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
<td>30</td>
<td>54</td>
<td>18</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
<td>30</td>
<td>54</td>
<td>18</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
<td>31</td>
<td>55</td>
<td>19</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
<td>32</td>
<td>55</td>
<td>19</td>
<td>29</td>
</tr>
<tr>
<td>Stack 1</td>
<td>bridge_x_51a</td>
<td>1</td>
<td>32</td>
<td>56</td>
<td>20</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>bridge_x_51b</td>
<td>2</td>
<td>32</td>
<td>56</td>
<td>20</td>
<td>26</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52a</td>
<td>1</td>
<td>33</td>
<td>57</td>
<td>21</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>bridge_x_52b</td>
<td>2</td>
<td>33</td>
<td>57</td>
<td>21</td>
<td>27</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53a</td>
<td>1</td>
<td>34</td>
<td>58</td>
<td>22</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>bridge_x_54b</td>
<td>2</td>
<td>34</td>
<td>58</td>
<td>22</td>
<td>30</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_ya</td>
<td>1</td>
<td>35</td>
<td>59</td>
<td>23</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>bridge_x_yb</td>
<td>2</td>
<td>35</td>
<td>59</td>
<td>23</td>
<td>31</td>
</tr>
</tbody>
</table>
### Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade switch models 6505, 6510, 6520, 7840, G610, G620, G630, and DCX 8510-8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Connects to FC_switch...</td>
</tr>
<tr>
<td>Stack 1</td>
<td>bridge_x_1a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1B</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_2a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td>bridge_x_2B</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_3a</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td>bridge_x_3B</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_ya</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td>bridge_x_yb</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
</tbody>
</table>

* - Ports 12 through 15 are reserved for the second MetroCluster or DR group on the Brocade 7840 switch.

**Note:** Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620 and G630 switches.
## Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade switch model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Connects to FC_switch...</td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
</tr>
<tr>
<td>Stack 1 bridge_x_51a</td>
<td>FC1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>2</td>
</tr>
<tr>
<td>bridge_x_51b</td>
<td>FC1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>2</td>
</tr>
</tbody>
</table>
Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade switch model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Connects to FC_switch...</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge_x_52</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge_x_53</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_5y</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge_x_5y</td>
<td>FC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
</tr>
</tbody>
</table>

**Note:** Additional bridges can be cabled to ports 36 to 39 in G620 and G630 switches.

### Brocade port usage for ISLs in a MetroCluster configuration running ONTAP 9.1 or later

The following table shows ISL port usage for the Brocade switches.

**Note:** AFF A700 or FAS9000 systems support up to eight ISLs for improved performance. Eight ISLs are supported on the Brocade 6510 and G620 switches.

<table>
<thead>
<tr>
<th>Switch model</th>
<th>ISL port</th>
<th>Switch port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade 6520</td>
<td>ISL port 1</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>ISL port 2</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>ISL port 3</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>ISL port 4</td>
<td>95</td>
</tr>
<tr>
<td>Brocade 6505</td>
<td>ISL port 1</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>ISL port 2</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>ISL port 3</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>ISL port 4</td>
<td>23</td>
</tr>
<tr>
<td>Switch model</td>
<td>ISL port</td>
<td>Switch port</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Brocade 6510 and Brocade DCX 8510-8</td>
<td>ISL port 1</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>ISL port 2</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>ISL port 3</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>ISL port 4</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>ISL port 5</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>ISL port 6</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>ISL port 7</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>ISL port 8</td>
<td>47</td>
</tr>
<tr>
<td>Brocade 7840</td>
<td>ISL port 1</td>
<td>ge0 (40-Gbps) or ge2 (10-Gbps)</td>
</tr>
<tr>
<td></td>
<td>ISL port 2</td>
<td>ge1 (40-Gbps) or ge3 (10-Gbps)</td>
</tr>
<tr>
<td></td>
<td>ISL port 3</td>
<td>ge10 (10-Gbps)</td>
</tr>
<tr>
<td></td>
<td>ISL port 4</td>
<td>ge11 (10-Gbps)</td>
</tr>
<tr>
<td>Brocade G10</td>
<td>ISL port 1</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>ISL port 2</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>ISL port 3</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>ISL port 4</td>
<td>23</td>
</tr>
<tr>
<td>Brocade G620 and Brocade G630</td>
<td>ISL port 1</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>ISL port 2</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>ISL port 3</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>ISL port 4</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>ISL port 5</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>ISL port 6</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>ISL port 7</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>ISL port 8</td>
<td>47</td>
</tr>
</tbody>
</table>

**Note:** The Brocade 7840 switch supports either two 40 Gbps VE-ports or up to four 10 Gbps VE-ports per switch for the creation of FCIP ISLs.

**Cisco port usage for controllers in a MetroCluster configuration running ONTAP 9.4 or later**

The tables show the maximum supported configuration, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules.
<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>52</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>53</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>54</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>55</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>56</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>56</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>26</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>27</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>28</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>28</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>29</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>30</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>31</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>32</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>32</td>
</tr>
<tr>
<td>Component</td>
<td>Port</td>
<td>Switch 1</td>
<td>Switch 2</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>MDS module 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDS module 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td></td>
<td>13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 9148 or 9250i*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td></td>
<td>13</td>
</tr>
</tbody>
</table>

* - The Cisco 9250i switch is not supported for eight-node MetroCluster configurations.
Cisco port usage for FC-to-SAS bridges in a MetroCluster configuration running ONTAP 9.1 or later

<table>
<thead>
<tr>
<th>FibreBridge 7500 using two FC ports</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>16</td>
</tr>
</tbody>
</table>

Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.

<table>
<thead>
<tr>
<th>FibreBridge 7500 using two FC ports</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>13</td>
</tr>
</tbody>
</table>
## Cisco 9148S

<table>
<thead>
<tr>
<th>FibreBridge 7500 using two FC ports</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>16</td>
</tr>
</tbody>
</table>

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 33 through 40 following the same pattern.

## Cisco 9132T

<table>
<thead>
<tr>
<th>FibreBridge 7500 using two FC ports</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>12</td>
</tr>
</tbody>
</table>

Additional bridges for a second DR group or second MetroCluster configuration can be attached using the same port numbers on the second MDS module.

## Cisco 9148 or 9250i

<table>
<thead>
<tr>
<th>FibreBridge 7500 using two FC ports</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>17</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>17</td>
</tr>
</tbody>
</table>
The following tables show bridge port usage when using FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port (FC1 or FC2) only. For FibreBridge 7500 bridges using one FC port, either FC1 or FC2 can be cabled to the port indicated as FC1. Additional bridges can be attached using ports 25-48.

### Cisco 9148 or 9250i

<table>
<thead>
<tr>
<th>FibreBridge 7500 using two FC ports</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>18</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>19</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>21</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>22</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>23</td>
</tr>
</tbody>
</table>

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.

### FibreBridge 6500 bridge or FibreBridge 7500 using one FC port

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge or FibreBridge 7500 using one FC port</th>
<th>Port</th>
<th>Cisco 9396S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Switch 1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>16</td>
</tr>
<tr>
<td>FibreBridge 6500 bridge or FibreBridge 7500 using one FC port</td>
<td>Port</td>
<td>Cisco 9396S</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>Switch 1</td>
</tr>
<tr>
<td>Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge or FibreBridge 7500 using one FC port</th>
<th>Port</th>
<th>Cisco 9148S</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>Switch 1</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>16</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td>Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco 9148 or 9250i</th>
<th>FibreBridge 6500 bridge or FibreBridge 7500 using one FC port</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>17</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
### Cisco 9148 or 9250i

<table>
<thead>
<tr>
<th>FibreBridge 6500 bridge or FibreBridge 7500 using one FC port</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
<td>17</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>18</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
<td>18</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>19</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
<td>19</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>21</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
<td>21</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>22</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
<td>22</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>23</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
<td>23</td>
</tr>
</tbody>
</table>

Additional bridges can be attached using ports 25 through 48 following the same pattern.

### Cisco port usage for ISLs in an eight-node configuration in a MetroCluster configuration running ONTAP 9.1 or later

The following table shows ISL port usage. ISL port usage is the same on all switches in the configuration.

<table>
<thead>
<tr>
<th>Switch model</th>
<th>ISL port</th>
<th>Switch port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 9396S</td>
<td>ISL 1</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>ISL 2</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>ISL 3</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>ISL 4</td>
<td>96</td>
</tr>
<tr>
<td>Cisco 9148 with 24 port license or 9250i</td>
<td>ISL 1</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>ISL 2</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>ISL 3</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>ISL 4</td>
<td>24</td>
</tr>
<tr>
<td>Cisco 9148, 9148S</td>
<td>ISL 1</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>ISL 2</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>ISL 3</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>ISL 4</td>
<td>48</td>
</tr>
<tr>
<td>Switch model</td>
<td>ISL port</td>
<td>Switch port</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Cisco 9132T</td>
<td>ISL 1</td>
<td>MDS module 1 port 13</td>
</tr>
<tr>
<td></td>
<td>ISL 2</td>
<td>MDS module 1 port 14</td>
</tr>
<tr>
<td></td>
<td>ISL 3</td>
<td>MDS module 1 port 15</td>
</tr>
<tr>
<td></td>
<td>ISL 4</td>
<td>MDS module 1 port 16</td>
</tr>
</tbody>
</table>
Using the Interoperability Matrix Tool to find MetroCluster information

When setting up the MetroCluster configuration, you can use the Interoperability Tool to ensure you are using supported software and hardware versions.

NetApp Interoperability Matrix Tool

After opening the Interoperability Matrix, you can use the Storage Solution field to select your MetroCluster solution.

You use the Component Explorer to select the components and ONTAP version to refine your search.

You can click Show Results to display the list of supported configurations that match the criteria.
You can learn more about configuring, operating, and monitoring a MetroCluster configuration in NetApp's extensive documentation library.

**MetroCluster and miscellaneous guides**

<table>
<thead>
<tr>
<th>Guide</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ONTAP 9 Documentation Center</strong></td>
<td>• All MetroCluster guides</td>
</tr>
<tr>
<td></td>
<td>• Best practices for MetroCluster configuration.</td>
</tr>
<tr>
<td><strong>Fabric-attached MetroCluster installation and configuration</strong></td>
<td>• Fabric-attached MetroCluster architecture</td>
</tr>
<tr>
<td></td>
<td>• Cabling the configuration</td>
</tr>
<tr>
<td></td>
<td>• Configuring the FC-to-SAS bridges</td>
</tr>
<tr>
<td></td>
<td>• Configuring the FC switches</td>
</tr>
<tr>
<td></td>
<td>• Configuring the MetroCluster in ONTAP</td>
</tr>
<tr>
<td><strong>Stretch MetroCluster installation and configuration</strong></td>
<td>• Stretch MetroCluster architecture</td>
</tr>
<tr>
<td></td>
<td>• Cabling the configuration</td>
</tr>
<tr>
<td></td>
<td>• Configuring the FC-to-SAS bridges</td>
</tr>
<tr>
<td></td>
<td>• Configuring the MetroCluster in ONTAP</td>
</tr>
<tr>
<td><strong>MetroCluster IP installation and configuration</strong></td>
<td>• MetroCluster IP architecture</td>
</tr>
<tr>
<td></td>
<td>• Cabling the configuration</td>
</tr>
<tr>
<td></td>
<td>• Configuring the MetroCluster in ONTAP</td>
</tr>
<tr>
<td><strong>Active IQ Unified Manager documentation</strong></td>
<td>• Monitoring the MetroCluster configuration and performance</td>
</tr>
<tr>
<td><strong>NetApp Documentation: Product Guides and Resources</strong></td>
<td>• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software</td>
</tr>
<tr>
<td><strong>MetroCluster Tiebreaker Software Installation and Configuration Guide</strong></td>
<td>• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software</td>
</tr>
<tr>
<td><strong>7-Mode Transition Tool 3.3.1 Copy-Based Transition Guide</strong></td>
<td>• Transitioning data from 7-Mode storage systems to clustered storage systems</td>
</tr>
</tbody>
</table>
Copyright

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277