ONTAP® 9

Fabric-attached MetroCluster® Installation and Configuration Guide

July 2019 | 215-11162_U0
doccomments@netapp.com
Updated for ONTAP 9.6
Contents

Deciding whether to use this guide ............................................................. 8
Preparing for the MetroCluster installation .............................................. 9
  Differences between the ONTAP MetroCluster configurations ................... 9
  Considerations for configuring cluster peering ........................................ 10
    Prerequisites for cluster peering .......................................................... 10
    Considerations when using dedicated ports ........................................... 11
    Considerations when sharing data ports ................................................. 11
  Considerations for MetroCluster configurations with native disk shelves or
    array LUNs ........................................................................................ 12
  Considerations when transitioning from 7-Mode to ONTAP .......................... 12
  Considerations for ISLs .......................................................................... 12
  Considerations for using TDM/WDM equipment with fabric-attached
    MetroCluster configurations ................................................................. 14
  Requirements for using a Brocade DCX 8510-8 switch ............................. 15
  Considerations when using unmirrored aggregates .................................... 16
  Preconfigured settings for new MetroCluster systems from the factory .......... 17
    Hardware setup checklist .................................................................... 17
Choosing the correct installation procedure for your configuration ......... 20
Cabling a fabric-attached MetroCluster configuration .............................. 21
  Parts of a fabric MetroCluster configuration ........................................... 22
    Illustration of the local HA pairs in a MetroCluster configuration ............. 26
    Illustration of redundant FC-to-SAS bridges ....................................... 27
    Redundant FC switch fabrics .............................................................. 27
    Illustration of the cluster peering network ......................................... 28
  Required MetroCluster FC components and naming conventions .............. 29
  Configuration worksheet for FC switches and FC-to-SAS bridges .............. 32
Installing and cabling MetroCluster components ..................................... 34
  Racking the hardware components ........................................................ 34
    Cabling the new controller module's FC-VI and HBA ports to the FC
      switches ....................................................................................... 35
    Cabling the ISLs between MetroCluster sites ...................................... 35
    Port assignments for systems using two initiator ports ....................... 36
    Port assignments for FC switches when using ONTAP 9.0 ..................... 37
    Port assignments for FC switches when using ONTAP 9.1 and later .......... 52
    Cabling the cluster interconnect in eight- or four-node configurations ...... 68
    Cabling the cluster peering connections .......................................... 69
    Cabling the HA interconnect, if necessary ....................................... 69
    Cabling the management and data connections .................................. 70
  Configuring the FC switches .................................................................. 70
    Configuring the FC switches by running a configuration file ............... 70
    Configuring the Cisco or Brocade FC switches manually .................... 72
Configuring ONTAP on a system that uses only array LUNs .......................... 263
Setting up the cluster ................................................................. 266
Installing the license for using array LUNs in a MetroCluster configuration ................ 266
Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems ......................................................... 267
Assigning ownership of array LUNs ............................................ 268
Peering the clusters ................................................................. 269
Mirroring the root aggregates .................................................. 269
Creating data aggregates on, implementing, and verifying the MetroCluster configuration ........................................ 270
Implementing a MetroCluster configuration with both disks and array LUNs .......... 271
Considerations when implementing a MetroCluster configuration with disks and array LUNs .................................................. 271
Example of a two-node fabric-attached MetroCluster configuration with disks and array LUNs .................................................. 272
Example of a four-node MetroCluster configuration with disks and array LUNs .................................................. 275
Using the Active IQ Unified Manager and ONTAP System Manager for further configuration and monitoring ........................................ 278
Synchronizing the system time using NTP .................................................. 278
Considerations when using ONTAP in a MetroCluster configuration .................................................. 279
FlexGroup support in MetroCluster configurations ........................................ 279
Job schedules in a MetroCluster configuration ........................................ 279
Cluster peering from the MetroCluster site to a third cluster .......................... 279
LDAP client configuration replication in a MetroCluster configuration .............. 279
Networking and LIF creation guidelines for MetroCluster configurations ............ 280
IPspace object replication and subnet configuration requirements ...................... 280
Requirements for LIF creation in a MetroCluster configuration ...................... 281
LIF replication and placement requirements and issues ...................................... 281
Volume creation on a root aggregate ................................................. 284
SVM disaster recovery in a MetroCluster configuration .................................... 284
SVM resynchronization at a disaster recovery site .......................................... 286
Output for the storage aggregate plex show command is indeterminate after a MetroCluster switchover .................................................. 286
Modifying volumes to set the NVFAIL flag in case of switchover .................... 287
Monitoring and protecting the file system consistency using NVFAIL ............... 287
How NVFAIL impacts access to NFS volumes or LUNs .................................... 287
Commands for monitoring data loss events ................................................. 288
Accessing volumes in NVFAIL state after a switchover ................................. 289
Recovering LUNs in NVFAIL states after switchover ....................................... 289
Where to find additional information .................................................. 290
Copyright ...................................................................................... 292
Trademark ...................................................................................... 293
How to send comments about documentation and receive update notifications ................................................................. 294
Deciding whether to use the Fabric-attached MetroCluster Installation and Configuration Guide

This guide describes how to install and configure the MetroCluster hardware and software components in a fabric configuration.

You should use this guide for planning, installing, and configuring a fabric-attached MetroCluster configuration under the following circumstances:

• You want to understand the architecture of a fabric-attached MetroCluster configuration.
• You want to understand the requirements and best practices for configuring a fabric-attached MetroCluster configuration.
• You want to use the command-line interface (CLI), not an automated scripting tool.

You can find other MetroCluster documentation in the following location:

ONTAP 9 Documentation Center
### Preparing for the MetroCluster installation

As you prepare for the MetroCluster installation, you should understand the MetroCluster hardware architecture and required components.

### Differences between the ONTAP MetroCluster configurations

The various MetroCluster configurations have key differences in the required components.

In all configurations, each of the two MetroCluster sites is configured as an ONTAP cluster. In a two-node MetroCluster configuration, each node is configured as a single-node cluster.

<table>
<thead>
<tr>
<th>Feature</th>
<th>IP configurations</th>
<th>Fabric-attached configurations</th>
<th>Stretch configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Four or eight-node</td>
<td>Two-node</td>
</tr>
<tr>
<td>Number of controllers</td>
<td>Four</td>
<td>Four or eight</td>
<td>Two</td>
</tr>
<tr>
<td>Uses an FC switch</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses an IP switch</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Uses an IP switch</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Uses FC-to-SAS bridges</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses direct-attached SAS storage</td>
<td>Yes (local attached only)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports ADP</td>
<td>Yes (starting in ONTAP 9.4)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports local HA</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Supports automatic switchover</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports unmirrored aggregates</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports array LUNs</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Considerations for configuring cluster peering

Each MetroCluster site is configured as a peer to its partner site. You should be familiar with the prerequisites and guidelines for configuring the peering relationships and when deciding whether to use shared or dedicated ports for those relationships.

Related information

Cluster and SVM peering express configuration

Prerequisites for cluster peering

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

Connectivity requirements

Every intercluster LIF on the local cluster must be able to communicate with every intercluster LIF on the remote cluster.

Although it is not required, it is typically simpler to configure the IP addresses used for intercluster LIFs in the same subnet. The IP addresses can reside in the same subnet as data LIFs, or in a different subnet. The subnet used in each cluster must meet the following requirements:

- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node. For example, in a six-node cluster, the subnet used for intercluster communication must have six available IP addresses.

Each node must have an intercluster LIF with an IP address on the intercluster network.

Intercluster LIFs can have an IPv4 address or an IPv6 address.

Note: ONTAP 9 enables you to migrate your peering networks from IPv4 to IPv6 by optionally allowing both protocols to be present simultaneously on the intercluster LIFs. In earlier releases, all intercluster relationships for an entire cluster were either IPv4 or IPv6. This meant that changing protocols was a potentially disruptive event.

Port requirements

You can use dedicated ports for intercluster communication, or share ports used by the data network. Ports must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace. You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.
- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port.
- Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).
- All ports must be cabled.
- All ports must be in a healthy state.
- The MTU settings of the ports must be consistent.

Firewall requirements

Firewalls and the intercluster firewall policy must allow the following protocols:

- ICMP service
• TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
• Bidirectional HTTPS between the intercluster LIFs

Although HTTPS is not required when you set up cluster peering using the CLI, HTTPS is required later if you use ONTAP System Manager to configure data protection.

The default intercluster firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0). You can modify or replace the policy if necessary.

Considerations when using dedicated ports

When determining whether using a dedicated port for intercluster replication is the correct intercluster network solution, you should consider configurations and requirements such as LAN type, available WAN bandwidth, replication interval, change rate, and number of ports.

Consider the following aspects of your network to determine whether using a dedicated port is the best intercluster network solution:

• If the amount of available WAN bandwidth is similar to that of the LAN ports and the replication interval is such that replication occurs while regular client activity exists, then you should dedicate Ethernet ports for intercluster replication to avoid contention between replication and the data protocols.
• If the network utilization generated by the data protocols (CIFS, NFS, and iSCSI) is such that the network utilization is above 50 percent, then you should dedicate ports for replication to allow for nondegraded performance if a node failover occurs.
• When physical 10 GbE or faster ports are used for data and replication, you can create VLAN ports for replication and dedicate the logical ports for intercluster replication. The bandwidth of the port is shared between all VLANs and the base port.
• Consider the data change rate and replication interval and whether the amount of data that must be replicated on each interval requires enough bandwidth that it might cause contention with data protocols if sharing data ports.

Considerations when sharing data ports

When determining whether sharing a data port for intercluster replication is the correct intercluster network solution, you should consider configurations and requirements such as LAN type, available WAN bandwidth, replication interval, change rate, and number of ports.

Consider the following aspects of your network to determine whether sharing data ports is the best intercluster connectivity solution:

• For a high-speed network, such as a 40-Gigabit Ethernet (40-GbE) network, a sufficient amount of local LAN bandwidth might be available to perform replication on the same 40-GbE ports that are used for data access. In many cases, the available WAN bandwidth is far less than 10 GbE LAN bandwidth.
• All nodes in the cluster might have to replicate data and share the available WAN bandwidth, making data port sharing more acceptable.
• Sharing ports for data and replication eliminates the extra port counts required to dedicate ports for replication.
• The maximum transmission unit (MTU) size of the replication network will be the same size as that used on the data network.
• Consider the data change rate and replication interval and whether the amount of data that must be replicated on each interval requires enough bandwidth that it might cause contention with data protocols if sharing data ports.
• When data ports for intercluster replication are shared, the intercluster LIFs can be migrated to any other intercluster-capable port on the same node to control the specific data port that is used for replication.

Considerations for MetroCluster configurations with native disk shelves or array LUNs

The MetroCluster configuration supports installations with native (NetApp) disk shelves only, array LUNs only, or a combination of both.
AFF systems do not support array LUNs.

Related concepts
Planning and installing a MetroCluster configuration with array LUNs on page 232

Related tasks
Cabling a fabric-attached MetroCluster configuration on page 21

Related information
FlexArray virtualization installation requirements and reference

Considerations when transitioning from 7-Mode to ONTAP

You must have the new MetroCluster configuration fully configured and operating before you use the transition tools to move data from a 7-Mode MetroCluster configuration to an ONTAP configuration.
If the 7-Mode configuration uses Brocade 6510 switches, the new configuration can share the existing fabrics to reduce the hardware requirements.
If you have Brocade 6510 switches and plan on sharing the switch fabrics between the 7-Mode fabric MetroCluster and the MetroCluster running in ONTAP, you must use the specific procedure for configuring the MetroCluster components.
FMC-MCC transition: Configuring the MetroCluster hardware for sharing a 7-Mode Brocade 6510 FC fabric during transition on page 165

Considerations for ISLs

You must determine how many ISLs you need for each FC switch fabric in the MetroCluster configuration. Beginning with ONTAP 9.2, in some cases, instead of dedicating FC switches and ISLs to each individual MetroCluster configuration, you can share the same four switches.

ISL sharing considerations (ONTAP 9.2)
Starting with ONTAP 9.2, you can use ISL sharing in the following cases:
• One two-node and one four-node MetroCluster configurations
• Two separate four-node MetroCluster configurations
• Two separate two-node MetroCluster configurations
• Two DR groups within one eight-node MetroCluster configuration
The number of ISLs required between the shared switches depends on the bandwidth of the platform models connected to the shared switches.

Consider the following aspects of your configuration when determining how many ISLs you need.

- Non-MetroCluster devices should not be connected to any of the FC switches that provide the back-end MetroCluster connectivity.
- ISL sharing is supported on all switches except the Cisco 9250i and Cisco 9148 switches.
- All nodes must be running ONTAP 9.2 or later.
- The FC switch cabling for ISL sharing is the same as for the eight-node MetroCluster cabling.
- The RCF files for ISL sharing are same as for the eight-node MetroCluster cabling.
- You should verify that all hardware and software versions are supported.

NetApp Hardware Universe

- The speed and number of ISLs must be sized to support the client load on both MetroCluster systems.
- The back-end ISLs and the back-end components must be dedicated to the MetroCluster configuration only.
- The ISL must use one of the supported speeds: 4 Gbps, 8 Gbps, 16 Gbps, or 32 Gbps.
- The ISLs on one fabric should all be the same speed and length.
- The ISLs on one fabric should all have the same topology. For example, they should all be direct links, or if your system uses WDM, then they should all use WDM.

Platform-specific ISL considerations

The number of recommended ISLs is platform-model specific. The following table shows the ISL requirements for each fabric by platform model. It assumes that each ISL has a 16-Gbps capacity.

<table>
<thead>
<tr>
<th>Platform model</th>
<th>Recommended number of ISLs per four-node DR group (per switch fabric)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFF A700</td>
<td>Six</td>
</tr>
<tr>
<td>FAS9000</td>
<td>Six</td>
</tr>
<tr>
<td>8080</td>
<td>Four</td>
</tr>
<tr>
<td>All others</td>
<td>Two</td>
</tr>
</tbody>
</table>

If the switch fabric is supporting eight nodes (either part of a single, eight-node MetroCluster configuration, or two four-node configurations that are sharing ISLs), the recommended total number of ISLs for the fabric is the sum of that required for each four-node DR group. For example:

- If DR group 1 includes four AFF A700 systems, it requires six ISLs.
- If DR group 2 includes four FAS8200 systems, it requires two ISLs.
- The total number of recommended ISLs for the switch fabric is eight.
Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations

The Hardware Universe tool provides some notes about the requirements that Time Division Multiplexing (TDM) or Wavelength Division Multiplexing (WDM) equipment must meet to work with a fabric-attached MetroCluster configuration. These notes also include information about various configurations, which can help you to determine when to use in-order delivery (IOD) of frames or out-of-order delivery (OOD) of frames.

An example of such requirements is that the TDM/WDM equipment must support the link aggregation (trunking) feature with routing policies. The order of delivery (IOD or OOD) of frames is maintained within a switch, and is determined by the routing policy that is in effect.

NetApp Hardware Universe

The following table provides the routing policies for configurations containing Brocade switches and Cisco switches:

<table>
<thead>
<tr>
<th>Switches</th>
<th>Configuring MetroCluster configurations for IOD</th>
<th>Configuring MetroCluster configurations for OOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade</td>
<td>• AptPolicy must be set to 1</td>
<td>• AptPolicy must be set to 3</td>
</tr>
<tr>
<td></td>
<td>• DLS must be set to off</td>
<td>• DLS must be set to on</td>
</tr>
<tr>
<td></td>
<td>• IOD must be set to on</td>
<td>• IOD must be set to off</td>
</tr>
<tr>
<td>Cisco</td>
<td>Policies for the FCVI-designated VSAN:</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>• Load balancing policy: srcid and dstid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IOD must be set to on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policies for the storage-designated VSAN:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Load balancing policy: srcid, dstid, and oxid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VSAN must not have the in-order-guarantee</td>
<td></td>
</tr>
<tr>
<td></td>
<td>option set</td>
<td></td>
</tr>
</tbody>
</table>

When to use IOD

It is best to use IOD if it is supported by the links. The following configurations support IOD:

- A single ISL
- The ISL and the link (and the link equipment, such as TDM/WDM, if used) supports configuration for IOD.
- A single trunk, and the ISLs and the links (and the link equipment, such as TDM/WDM, if used) support configuration for IOD.

When to use OOD

- You can use OOD for all configurations that do not support IOD.
• You can use OOD for configurations that do not support the trunking feature.

Using encryption devices

When using dedicated encryption devices on the ISL or encryption on WDM devices in the MetroCluster configuration, you must meet the following requirements:

• The external encryption devices or WDM equipment has been self certified by the vendor with the FC switch in question. The self certification should cover the operating mode (such as trunking and encryption).
• The added latency due to encryption should be no more than 10 microseconds.

Requirements for using a Brocade DCX 8510-8 switch

• The DCX 8510-8 switches used in MetroCluster configurations must be purchased from NetApp.
• For scalability, you should leave one port-chunk between MetroCluster configurations if cabling only two MetroClusters in 4x48-port modules. This enables you to expand port usage in MetroCluster configurations without recabling.
• Each Brocade DCX 8510-8 switch in the MetroCluster configuration must be correctly configured for the ISL ports and storage connections. For port usage, see the following section: Port assignments for FC switches when using ONTAP 9.1 and later on page 52.
• ISLs cannot be shared and each MetroCluster requires two ISLs for each fabric.
• The DCX 8510-8 switch used for backend MetroCluster connectivity should not be used for any other connectivity. Non-MetroCluster devices should not be connected to these switches and non-MetroCluster traffic should not flow through DCX 8510-8 switches.
• One line card can either be connected to ONTAP MetroClusters or ONTAP 7-Mode MetroClusters.

Note: RCF files are not available for this switch.

The following are the requirements for using two Brocade DCX 8510-8 switches:

• You must have one DCX 8510-8 switch at each site.
• You must use a minimum of two 48-port blades that contain 16Gb SFPs in each switch.

The following are the requirements for using four DCX 8510-8 switches at each site in a MetroCluster configuration:

• You must have two DCX 8510-8 switches at each site.
• You must use at least one 48-port blade for each DCX 8510-8 switch.
• Each blade is configured as a virtual switch using virtual fabrics.

The following NetApp products are not supported by Brocade DCX 8510-8 switches:

• Config Advisor
• Fabric Health Monitor
• MyAutoSupport (system risks might show false positives)
• Active IQ Unified Manager (formerly OnCommand Unified Manager)
Note:
Ensure that all the components needed for this configuration are in the Interoperability Matrix Tool. Read the notes section in the Interoperability Matrix Tool for information on supported configurations.

NetApp Interoperability Matrix Tool

Considerations when using unmirrored aggregates

If your configuration includes unmirrored aggregates, you must be aware of potential access issues after switchover operations.

Considerations for unmirrored aggregates when doing maintenance requiring power shutdown

If you are performing negotiated switchover for maintenance reasons requiring site-wide power shutdown, you should first manually take offline any unmirrored aggregates owned by the disaster site.

If you do not, nodes at the surviving site might go down due to multi-disk panics. This could occur if switched-over unmirrored aggregates go offline or are missing because of the loss of connectivity to storage at the disaster site due to the power shutdown or a loss of ISLs.

Considerations for unmirrored aggregates and hierarchical namespaces

If you using hierarchical namespaces, you should configure the junction path so that all of the volumes in that path are either on mirrored aggregates only or on unmirrored aggregates only. Configuring a mix of unmirrored and mirrored aggregates in the junction path might prevent access to the unmirrored aggregates after the switchover operation.

Considerations for unmirrored aggregates and CRS MDV and data SVM's root volumes

The configuration replication service (CRS) metadata volume and data SVM's root volumes must be on a mirrored aggregate. You cannot move these volumes to unmirrored aggregate. If they are on unmirrored aggregate, negotiated switchover and switchback operations are vetoed. The metrocluster check command provides a warning if this is the case.

Considerations for unmirrored aggregates and SVMs using SAN protocols

SVMs configured for SAN protocols should be configured on mirrored aggregates only or on unmirrored aggregates only. Configuring a mix of unmirrored and mirrored aggregates can result in a switchover operation that exceeds 120 seconds and result in a data outage if the unmirrored aggregates do not come online.
Preconfigured settings for new MetroCluster systems from the factory

New MetroCluster nodes, FC-to-SAS bridges, and FC switches are preconfigured and MetroCluster settings are enabled in the software. In most cases, you do not need to perform the detailed procedures provided in this guide.

Hardware racking and cabling

Depending on the configuration you ordered, you might need to rack the systems and complete the cabling.

*Configuring the MetroCluster hardware components in systems with native disk shelves* on page 21

FC switch and FC-to-SAS bridge configurations

For configurations using FC-to-SAS bridges, the bridges received with the new MetroCluster configuration are preconfigured and do not require additional configuration unless you want to change the names and IP addresses.

For configurations using FC switches, in most cases, FC switch fabrics received with the new MetroCluster configuration are preconfigured for two Inter-Switch Links (ISLs). If you are using additional ISLs, you must manually configure the switches.

*Configuring the FC switches* on page 70

Software configuration of the MetroCluster configuration

Nodes received with the new MetroCluster configuration are preconfigured with a single root aggregate. Additional configuration must be performed using the detailed procedures provided in this guide.

Hardware setup checklist

You need to know which hardware setup steps were completed at the factory and which steps you need to complete at each MetroCluster site.

<table>
<thead>
<tr>
<th>Step</th>
<th>Completed at factory</th>
<th>Completed by you</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount components in one or more cabinets.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Position cabinets in the desired location.</td>
<td>No</td>
<td>Yes Position them in the original order so that the supplied cables are long enough.</td>
</tr>
<tr>
<td>Connect multiple cabinets to each other, if applicable.</td>
<td>No</td>
<td>Yes Use the cabinet interconnect kit if it is included in the order. The kit box is labeled.</td>
</tr>
<tr>
<td>Secure the cabinets to the floor, if applicable.</td>
<td>No</td>
<td>Yes Use the universal bolt-down kit if it is included in the order. The kit box is labeled.</td>
</tr>
<tr>
<td>Step</td>
<td>Completed at factory</td>
<td>Completed by you</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Cable the components within the cabinet.</td>
<td>Yes Cables 5 meters and longer are removed for shipping and placed in the accessories box.</td>
<td>No</td>
</tr>
<tr>
<td>Connect the cables between cabinets, if applicable.</td>
<td>No</td>
<td>Yes Cables are in the accessories box.</td>
</tr>
<tr>
<td>Connect management cables to the customer's network.</td>
<td>No</td>
<td>Yes Connect them directly or through the CN1601 management switches, if present. <strong>Attention:</strong> To avoid address conflicts, do not connect management ports to the customer's network until after you change the default IP addresses to the customer's values.</td>
</tr>
<tr>
<td>Connect console ports to the customer's terminal server, if applicable.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect the customer's data cables to the cluster.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect the long-distance ISLs between the MetroCluster sites, if applicable.</td>
<td>No</td>
<td>Yes <strong>Cabling the ISLs between MetroCluster sites</strong> on page 35</td>
</tr>
<tr>
<td>Connect the cabinets to power and power on the components.</td>
<td>No</td>
<td>Yes Power them on in the following order: 1. PDUs 2. Disk shelves and FC-to-SAS bridges, if applicable 3. FC switches 4. Nodes</td>
</tr>
<tr>
<td>Assign IP addresses to the management ports of the cluster switches and to the management ports of the management switches, if present.</td>
<td>No</td>
<td>Yes, for switched clusters only Connect to the serial console port of each switch and log in with user name “admin” with no password. Suggested management addresses are 10.10.10.81, 10.10.10.82, 10.10.10.83, and 10.10.10.84.</td>
</tr>
</tbody>
</table>
### Step 2: Verify cabling by running the Config Advisor tool.

<table>
<thead>
<tr>
<th>Step</th>
<th>Completed at factory</th>
<th>Completed by you</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify cabling by running the Config Advisor tool.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Choosing the correct installation procedure for your configuration

You must choose the correct installation procedure based on whether you are using FlexArray LUNs, the number of nodes in the MetroCluster configuration, and whether you are sharing an existing FC switch fabric used by a 7-Mode fabric MetroCluster.

### For this installation type... | Use these procedures...
--- | ---
Fabric-attached configuration with NetApp (native) disks | 1. *Cabling a fabric-attached MetroCluster configuration* on page 21  
2. *Configuring the MetroCluster software in ONTAP* on page 173

Fabric-attached configuration when sharing with an existing FC switch fabric  
This is supported only as a temporary configuration with a 7-Mode fabric MetroCluster configuration using Brocade 6510 switches. | 1. *Cabling a fabric-attached MetroCluster configuration* on page 21  
2. *Configuring the MetroCluster hardware for sharing a 7-Mode Brocade 6510 FC fabric during transition* on page 165  
3. *Configuring the MetroCluster software in ONTAP* on page 173
Cabling a fabric-attached MetroCluster configuration

The MetroCluster components must be physically installed, cabled, and configured at both geographic sites. The steps are slightly different for a system with native disk shelves as opposed to a system with array LUNs.

About this task

Steps
1. Parts of a fabric MetroCluster configuration on page 22
2. Required MetroCluster FC components and naming conventions on page 29
3. Configuration worksheet for FC switches and FC-to-SAS bridges on page 32
4. Installing and cabling MetroCluster components on page 34
5. Configuring the FC switches on page 70
6. Installing FC-to-SAS bridges and SAS disk shelves on page 151
Parts of a fabric MetroCluster configuration

As you plan your MetroCluster configuration, you should understand the hardware components and how they interconnect.

Disaster Recovery (DR) groups

A fabric MetroCluster configuration consists of one or two DR groups, depending on the number of nodes in the MetroCluster configuration. Each DR group consists of four nodes.

- An eight-node MetroCluster configuration consists of two DR groups.
- A four-node MetroCluster configuration consists of one DR group.

The following illustration shows the organization of nodes in an eight-node MetroCluster configuration:

![Diagram of an eight-node MetroCluster configuration]

The following illustration shows the organization of nodes in a four-node MetroCluster configuration:
Key hardware elements

A MetroCluster configuration includes the following key hardware elements:

- **Storage controllers**
  The storage controllers are not connected directly to the storage but connect to two redundant FC switch fabrics.

- **FC-to-SAS bridges**
  The FC-to-SAS bridges connect the SAS storage stacks to the FC switches, providing bridging between the two protocols.

- **FC switches**
  The FC switches provide the long-haul backbone ISL between the two sites. The FC switches provide the two storage fabrics that allow data mirroring to the remote storage pools.

- **Cluster peering network**
  The cluster peering network provides connectivity for mirroring of the cluster configuration, which includes storage virtual machine (SVM) configuration. The configuration of all of the SVMs on one cluster is mirrored to the partner cluster.

Eight-node fabric MetroCluster configuration

An eight-node configuration consists of two clusters, one at each geographically separated site. cluster_A is located at the first MetroCluster site. cluster_B is located at the second MetroCluster site. Each site has one SAS storage stack. Additional storage stacks are supported, but only one is shown at each site. The HA pairs are configured as switchless clusters, without cluster interconnect switches. A switched configuration is supported, but is not shown.

An eight-node configuration includes the following connections:

- FC connections from each controller's HBAs and FC-VI adapters to each of the FC switches
- An FC connection from each FC-to-SAS bridge to an FC switch
- SAS connections between each SAS shelf and from the top and bottom of each stack to an FC-to-SAS bridge
• An HA interconnect between each controller in the local HA pair
  If the controllers support a single-chassis HA pair, the HA interconnect is internal, occurring
  through the backplane, meaning that an external interconnect is not required.

• Ethernet connections from the controllers to the customer-provided network that is used for
  cluster peering
  SVM configuration is replicated over the cluster peering network.

• A cluster interconnect between each controller in the local cluster

**Four-node fabric MetroCluster configuration**

The following illustration shows a simplified view of a four-node fabric MetroCluster configuration. For some connections, a single line represents multiple, redundant connections between the components. Data and management network connections are not shown.

The following illustration shows a more detailed view of the connectivity in a single MetroCluster cluster (both clusters have the same configuration):
Two-node fabric MetroCluster configuration

The following illustration shows a simplified view of a two-node fabric MetroCluster configuration. For some connections, a single line represents multiple, redundant connections between the components. Data and management network connections are not shown.

A two-node configuration consists of two clusters, one at each geographically separated site. cluster_A is located at the first MetroCluster site. cluster_B is located at the second MetroCluster site. Each site has one SAS storage stack. Additional storage stacks are supported, but only one is shown at each site.
**Note:** In a two-node configuration, the nodes are not configured as an HA pair.

The following illustration shows a more detailed view of the connectivity in a single MetroCluster cluster (both clusters have the same configuration):

A two-node configuration includes the following connections:

- FC connections between the FC-VI adapter on each controller module
- FC connections from each controller module's HBAs to the FC-to-SAS bridge for each SAS shelf stack
- SAS connections between each SAS shelf and from the top and bottom of each stack to an FC-to-SAS bridge
- Ethernet connections from the controllers to the customer-provided network that is used for cluster peering

SVM configuration is replicated over the cluster peering network.

**Illustration of the local HA pairs in a MetroCluster configuration**

In eight-node or four-node MetroCluster configurations, each site consists of storage controllers configured as one or two HA pairs. This allows local redundancy so that if one storage controller fails, its local HA partner can take over. Such failures can be handled without a MetroCluster switchover operation.

Local HA failover and giveback operations are performed with the storage failover commands, in the same manner as a non-MetroCluster configuration.
Illustration of redundant FC-to-SAS bridges

FC-to-SAS bridges provide protocol bridging between SAS attached disks and the FC switch fabric.

Redundant FC switch fabrics

Each switch fabric includes inter-switch links (ISLs) that connect the sites. Data is replicated from site-to-site over the ISL. Each switch fabric must be on different physical paths for redundancy.
Illustration of the cluster peering network

The two clusters in the MetroCluster configuration are peered through a customer-provided cluster peering network. Cluster peering supports the synchronous mirroring of storage virtual machines (SVMs, formerly known as Vservers) between the sites.

Intercluster LIFs must be configured on each node in the MetroCluster configuration, and the clusters must be configured for peering. The ports with the intercluster LIFs are connected to the customer-provided cluster peering network. Replication of the SVM configuration is carried out over this network through the Configuration Replication Service.

Related concepts

Considerations for configuring cluster peering on page 10

Related tasks

Cabling the cluster peering connections on page 69
Peering the clusters on page 196
Related information

Cluster and SVM peering express configuration

**Required MetroCluster FC components and naming conventions**

When planning your MetroCluster FC configuration, you must understand the required and supported hardware and software components. For convenience and clarity, you should also understand the naming conventions used for components in examples throughout the documentation. For example, one site is referred to as Site A and the other site is referred to as Site B.

**Supported software and hardware**

The hardware and software must be supported for the MetroCluster FC configuration.

*NetApp Hardware Universe*

When using AFF systems, all controller modules in the MetroCluster configuration must be configured as AFF systems.

*Note:* Long-wave SFPs are not supported in the MetroCluster storage switches. For a table of supported SFPs, see the MetroCluster Technical Report.


**Hardware redundancy in the MetroCluster FC configuration**

Because of the hardware redundancy in the MetroCluster FC configuration, there are two of each component at each site. The sites are arbitrarily assigned the letters A and B and the individual components are arbitrarily assigned the numbers 1 and 2.

**Requirement for two ONTAP clusters**

The fabric-attached MetroCluster FC configuration requires two ONTAP clusters, one at each MetroCluster site.

Naming must be unique within the MetroCluster configuration.

Example names:

- Site A: cluster_A
- Site B: cluster_B

**Requirement for four FC switches**

The fabric-attached MetroCluster FC configuration requires four FC switches (supported Brocade or Cisco models).

The four switches form two switch storage fabrics that provide the ISL between each of the clusters in the MetroCluster FC configuration.

Naming must be unique within the MetroCluster configuration.

**Requirement for two, four, or eight controller modules**

The fabric-attached MetroCluster FC configuration requires two, four, or eight controller modules.

In a four or eight-node MetroCluster configuration, the controller modules at each site form one or two HA pairs. Each controller module has a DR partner at the other site.
The controller modules must meet the following requirements:

- Naming must be unique within the MetroCluster configuration.
- All controller modules in the MetroCluster configuration must be running the same version of ONTAP.
- All controller modules in a DR group must be of the same model. However, in configurations with two DR groups, each DR group can consist of different controller module models.
- All controller modules in a DR group must use the same FC-VI configuration. Some controller modules support two options for FC-VI connectivity:
  - Onboard FC-VI ports
  - An FC-VI card in slot 1

A mix of one controller module using onboard FC-VI ports and another using an add-on FC-VI card is not supported. For example, if one node uses onboard FC-VI configuration, then all other nodes in the DR group must use onboard FC-VI configuration as well.

Example names:

- Site A: controller_A_1
- Site B: controller_B_1

**Requirement for four cluster interconnect switches**

The fabric-attached MetroCluster FC configuration requires four cluster interconnect switches (if you are not using two-node switchless clusters).

These switches provide cluster communication among the controller modules in each cluster. The switches are not required if the controller modules at each site are configured as a two-node switchless cluster.

**Requirement for FC-to-SAS bridges**

The fabric-attached MetroCluster FC configuration requires one pair of FC-to-SAS bridges for each stack group of SAS shelves:

- FibreBridge 7600N or 7500N bridges support up to four SAS stacks.
- FibreBridge 6500N bridges support only one SAS stack.
- Each stack can use different models of IOM. A mix of IOM12 modules and IOM6/IOM3 modules is not supported within the same storage stack.
- Supported IOM modules depend on the version of ONTAP you are running.
- Naming must be unique within the MetroCluster configuration.

The suggested names used as examples in this guide identify the controller module and stack that the bridge connects to, as shown below.

**Pool and drive requirements (minimum supported)**

Eight SAS disk shelves are recommended (four shelves at each site) to allow disk ownership on a per-shelf basis.

The MetroCluster configuration requires the minimum configuration at each site:
Each node has at least one local pool and one remote pool at the site. For example, in a four-node MetroCluster configuration with two nodes at each site, four pools are required at each site.

At least seven drives in each pool. In a four-node MetroCluster configuration with a single mirrored data aggregate per node, the minimum configuration requires 28 disks at the site.

In a minimum supported configuration, each pool has the following drive layout:

- Three root drives
- Three data drives
- One spare drive

MetroCluster configurations support RAID-DP and RAID4.

**Drive location considerations for half-shelf configurations**

For correct auto-assignment of drives when using shelves that are half populated (12 drives in a 24-drive shelf), drives should be located in slots 0-5 and 18-23.

**Bridge naming conventions**

The bridges use the following example naming: bridge_\textit{site}_{stack} \textit{group}_{location} in pair

<table>
<thead>
<tr>
<th>This portion of the name...</th>
<th>Identifies the...</th>
<th>Possible values...</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{site}</td>
<td>Site on which the bridge pair physically resides.</td>
<td>A or B</td>
</tr>
<tr>
<td>\textit{stack group}</td>
<td>Number of the stack group to which the bridge pair connects.</td>
<td>1, 2, etc.</td>
</tr>
<tr>
<td>\textit{location in pair}</td>
<td>Bridge within the bridge pair. A pair of bridges connect to a specific stack group.</td>
<td>a or b</td>
</tr>
</tbody>
</table>

Example bridge names for one stack group on each site:

- bridge\textunderscore A\textunderscore 1a
- bridge\textunderscore A\textunderscore 1b
- bridge\textunderscore B\textunderscore 1a
- bridge\textunderscore B\textunderscore 1b
### Configuration worksheet for FC switches and FC-to-SAS bridges

Before beginning to configure the MetroCluster sites, you should gather required configuration information.

#### Site A, FC switch one (FC_switch_A_1)

<table>
<thead>
<tr>
<th>Switch configuration parameter</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1 IP address</td>
<td></td>
</tr>
<tr>
<td>FC_switch_A_1 Username</td>
<td></td>
</tr>
<tr>
<td>FC_switch_A_1 Password</td>
<td></td>
</tr>
</tbody>
</table>

#### Site A, FC switch two (FC_switch_A_2)

<table>
<thead>
<tr>
<th>Switch configuration parameter</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_2 IP address</td>
<td></td>
</tr>
<tr>
<td>FC_switch_A_2 Username</td>
<td></td>
</tr>
<tr>
<td>FC_switch_A_2 Password</td>
<td></td>
</tr>
</tbody>
</table>

#### Site A, FC-to-SAS bridge 1 (FC_bridge_A_1a)

Each SAS stack requires two FC-to-SAS bridges.

- For FibreBridge 7500N or 7600N bridges using both FC ports (FC1 and FC2), each bridge connects to FC_switch_A_1_port-number and FC_switch_A_2_port-number.
- For FibreBridge 6500N bridges or FibreBridge 7500N or 7600N bridges using one FC port (FC1 or FC2) only, one bridge connects to FC_switch_A_1_port-number and the second connects to FC_switch_A_2_port-number.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_A_1a IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1a Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1a Password</td>
<td></td>
</tr>
</tbody>
</table>

#### Site A, FC-to-SAS bridge 2 (FC_bridge_A_2_port-number)

Each SAS stack requires two FC-to-SAS bridges.
• For FibreBridge 7500N or 7600N bridges using both FC ports (FC1 and FC2), each bridge connects to FC_switch_A_1_port-number and FC_switch_A_2_port-number.

• For FibreBridge 6500N bridges or FibreBridge 7500N or 7600N bridges using one FC port (FC1 or FC2) only, one bridge connects to FC_switch_A_1_port-number and the second connects to FC_switch_A_2_port-number.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_A_1b IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1b Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1b Password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site B, FC switch one (FC_switch_B_1)</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_B_1 IP address</td>
<td></td>
</tr>
<tr>
<td>FC_switch_B_1 Username</td>
<td></td>
</tr>
<tr>
<td>FC_switch_B_1 Password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site B</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_B_2 IP address</td>
<td></td>
</tr>
<tr>
<td>FC_switch_B_2 Username</td>
<td></td>
</tr>
<tr>
<td>FC_switch_B_2 Password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site B, FC-to-SAS bridge 1 (FC_bridge_B_1a)</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_B_1a IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_1a Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_1a Password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site B</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_B_2a IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_2a Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_2a Password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site B, FC-to-SAS bridge 2 (FC_bridge_B_2b)</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_B_2b IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_2b Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_2b Password</td>
<td></td>
</tr>
</tbody>
</table>

Cabling a fabric-attached MetroCluster configuration | 33

• For FibreBridge 7500N or 7600N bridges using both FC ports (FC1 and FC2), each bridge connects to FC_switch_B_1_port-number and FC_switch_B_2_port-number.

• For FibreBridge 6500N bridges or FibreBridge 7500N or 7600N bridges using one FC port (FC1 or FC2) only, one bridge connects to FC_switch_B_1_port-number and the second connects to FC_switch_B_2_port-number.
• For FibreBridge 6500N bridges or FibreBridge 7500N or 7600N bridges using one FC port (FC1 or FC2) only, one bridge connects to FC_switch_B_1_port-number and the second connects to FC_switch_B_2_port-number.

<table>
<thead>
<tr>
<th>Site B</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_B_1b IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_1b Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_1b Password</td>
<td></td>
</tr>
</tbody>
</table>

Related information

*NetApp Interoperability Matrix Tool*

**Installing and cabling MetroCluster components**

The storage controllers must be cabled to the FC switches and the ISLs must be cabled to link the MetroCluster sites. The storage controllers must also be cabled to the cluster peering, data, and management networks.

**Steps**

1. **Racking the hardware components** on page 34
2. **Cabling the new controller module’s FC-VI and HBA ports to the FC switches** on page 35
3. **Cabling the ISLs between MetroCluster sites** on page 35
4. **Port assignments for systems using two initiator ports** on page 36
5. **Port assignments for FC switches when using ONTAP 9.0** on page 37
6. **Port assignments for FC switches when using ONTAP 9.1 and later** on page 52
7. **Cabling the cluster interconnect in eight- or four-node configurations** on page 68
8. **Cabling the cluster peering connections** on page 69
9. **Cabling the HA interconnect, if necessary** on page 69
10. **Cabling the management and data connections** on page 70

**Racking the hardware components**

If you have not received the equipment already installed in cabinets, you must rack the components.

**About this task**

This task must be performed on both MetroCluster sites.

**Steps**

1. **Plan out the positioning of the MetroCluster components.**
   The rack space depends on the platform model of the controller modules, the switch types, and the number of disk shelf stacks in your configuration.
2. **Properly ground yourself.**
3. **Install the controller modules in the rack or cabinet.**
4. **Install the FC switches in the rack or cabinet.**
5. Install the disk shelves, power them on, and then set the shelf IDs.

   NetApp Documentation: Disk Shelves

   • You must power-cycle each disk shelf.
   • Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (including both sites).

6. Install each FC-to-SAS bridge:

   a. Secure the “L” brackets on the front of the bridge to the front of the rack (flush-mount) with the four screws.

      The openings in the bridge “L” brackets are compliant with rack standard ETA-310-X for 19-inch (482.6 mm) racks.

      The ATTO FibreBridge Installation and Operation Manual for your bridge model contains more information and an illustration of the installation.

      Note: For adequate port space access and FRU serviceability, you must leave 1U space below the bridge pair and cover this space with a tool-less blanking panel.

   b. Connect each bridge to a power source that provides a proper ground.

   c. Power on each bridge.

      Note: For maximum resiliency, bridges that are attached to the same stack of disk shelves must be connected to different power sources.

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

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

The FC-VI ports and HBAs (host bus adapters) must be cabled to the site FC switches on each controller module in the MetroCluster configuration.

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 52
   • Port assignments for FC switches when using ONTAP 9.0 on page 37
   • Port assignments for systems using two initiator ports on page 36

Cabling the ISLs between MetroCluster sites

You must connect the FC switches at each site through the fiber-optic Inter-Switch Links (ISLs) to form the switch fabrics that connect the MetroCluster components.

About this task

This must be done for both switch fabrics.

Step

1. Connect the FC switches at each site to all ISLs, using the cabling in the table that corresponds to your configuration and switch model.
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.

MetroCluster Service Guide

The following table shows port assignments for FC switches when using ONTAP 9.1 and later.

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade switch models 6505, 6510, 6520, 7840, G620, G610, and DCX 8510-8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Connects to FC switch...</td>
<td>Connects to switch port...</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>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>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
<tr>
<td>Stack 1</td>
<td>bridge_x_1a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1b</td>
<td>2</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_ya</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>bridge_x_yb</td>
<td>2</td>
</tr>
</tbody>
</table>

The following table shows port assignments for FC switches when using ONTAP 9.0.
MetroCluster two-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></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC_switch_x_2</td>
<td>0</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>MetroCluster eight-node configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></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>controller_x_2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>controller_x_3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>controller_x_4</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<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>MetroCluster eight-node configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FibreBridge 7500 bridge</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_1a</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The following table shows bridge port usage when using FibreBridge 6500 bridges:

<table>
<thead>
<tr>
<th>MetroCluster eight-node configuration</th>
<th>Brocade 6505, 6510, or DCX 8510-8</th>
<th>FC_switch_x_1</th>
<th>FC_switch_x_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreBridge 7500 bridge</td>
<td>Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_1b</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_2a</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_2b</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_3a</td>
<td>FC1</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>17</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>17</td>
</tr>
<tr>
<td>bridge_x_4a</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_4b</td>
<td>FC1</td>
<td>19</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
<td>19</td>
</tr>
</tbody>
</table>

The following table shows bridge port usage when using FibreBridge 6500 bridges:

<table>
<thead>
<tr>
<th>MetroCluster eight-node configuration</th>
<th>Brocade 6505, 6510, or DCX 8510-8</th>
<th>FC_switch_x_1</th>
<th>FC_switch_x_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreBridge 6500 bridge</td>
<td>Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>17</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
<td>17</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>18</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
<td>18</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>19</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.

<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></td>
<td>FC_switch_x_1</td>
</tr>
<tr>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>2</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>3</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>MetroCluster four-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>
<tr>
<td>bridge_x_2b</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_3a</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_3b</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_4a</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_4b</td>
</tr>
<tr>
<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></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>
</tbody>
</table>
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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISL port</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>ISL port 1</td>
</tr>
<tr>
<td>ISL port 2</td>
</tr>
<tr>
<td>ISL port 3</td>
</tr>
<tr>
<td>ISL port 4</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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></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>
</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>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreBridge 7500 bridge</td>
<td>Port</td>
<td>FC_switch_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>FC2</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>FC2</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>MetroCluster two-node configuration</th>
<th>Brocade 6510, DCX 8510-8</th>
<th>Brocade 6505</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreBridge 6500 bridge</td>
<td>Port</td>
<td>FC_switch_1</td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>6</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>7</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>8</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_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

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:
## 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_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>
<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>
<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.

## MetroCluster eight-node configuration

<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>
</tbody>
</table>
### MetroCluster eight-node configuration

<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_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.

The following table shows bridge port usage up to port 23 when using FibreBridge 6500 bridges. Additional bridges can be attached using ports 25-48.

<table>
<thead>
<tr>
<th>FibreBridge 6500 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>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>
</tbody>
</table>
Cisco 9148 or 9148S

<table>
<thead>
<tr>
<th>Port</th>
<th>FC_switch_x_1</th>
<th>FC_switch_x_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge_x_8a</td>
<td>23</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8b</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 MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

<table>
<thead>
<tr>
<th>ISL port</th>
<th>MetroCluster eight-node configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_x_1</td>
<td>Cisco 9148 or 9148S</td>
</tr>
<tr>
<td>FC_switch_x_2</td>
<td>Cisco 9148 or 9148S</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:

<table>
<thead>
<tr>
<th>Component</th>
<th>MetroCluster four-node configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Cisco 9148, 9148S, or 9250i</td>
</tr>
<tr>
<td>FC_switch_x_1</td>
<td>Cisco 9148, 9148S, or 9250i</td>
</tr>
<tr>
<td>FC_switch_x_2</td>
<td>Cisco 9148, 9148S, or 9250i</td>
</tr>
<tr>
<td>controller_x_1</td>
<td>FC-VI port a</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
</tr>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
</tr>
</tbody>
</table>
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 four-node configuration</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>FibreBridge 7500 bridge</td>
<td></td>
<td></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>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>14</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>
</tbody>
</table>
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>36</th>
<th>36</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISL port 1</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>ISL port 2</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>ISL port 3</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>ISL port 4</td>
<td>48</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:
### MetroCluster two-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>FC_switch_x_1</td>
<td>FC_switch_x_2</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>
</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>
<tr>
<td>bridge_x_2b</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_3a</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_3b</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_4a</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bridge_x_4b</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 6500 bridge</th>
<th>Port</th>
<th>ISL port number</th>
</tr>
</thead>
<tbody>
<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>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>
<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

### MetroCluster 1 or DR Group 1

<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>Connects to FC switch...</td>
<td>Connects to switch port...</td>
</tr>
<tr>
<td>controller_x_1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC-VI port a</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>FC-VI port b</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>FC-VI port c</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FC-VI port d</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>HBA port a</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>HBA port b</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>HBA port c</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>HBA port d</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>controller_x_2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC-VI port a</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>FC-VI port b</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>FC-VI port c</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>FC-VI port d</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>HBA port a</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>HBA port b</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>HBA port c</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>HBA port d</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Stack 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_1a</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Stack 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Stack 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Stack y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge_x_ya</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_yb</td>
<td>2</td>
<td>11</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>MetroCluster 2 or DR Group 2</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Port</td>
<td>Connects to FC_switch...</td>
<td>Brocade switch model</td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
<td>27</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>1</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>Stack 1</td>
<td>bridge_x_51a</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>bridge_x_51b</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52a</td>
<td>1</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>bridge_x_52b</td>
<td>2</td>
<td>33</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53a</td>
<td>1</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>bridge_x_54b</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>Stack γ</td>
<td>bridge_x_γa</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>bridge_x_γb</td>
<td>2</td>
<td>35</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>controller_x_1</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_2</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</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>
</tbody>
</table>
## Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

### MetroCluster 1 or DR Group 1

<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 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)

### MetroCluster 2 or DR Group 2

<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>HBA port a</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td>HBA port b</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>HBA port c</td>
<td>1</td>
<td>27</td>
</tr>
<tr>
<td>HBA port d</td>
<td>2</td>
<td>27</td>
</tr>
</tbody>
</table>
## Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)  
### MetroCluster 2 or DR Group 2

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade switch model</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_4</td>
<td>FC-VI</td>
<td></td>
<td></td>
<td>1</td>
<td>28</td>
<td>52</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>port a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI</td>
<td></td>
<td></td>
<td>2</td>
<td>28</td>
<td>52</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>port b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI</td>
<td></td>
<td></td>
<td>1</td>
<td>29</td>
<td>53</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>port c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI</td>
<td></td>
<td></td>
<td>2</td>
<td>29</td>
<td>53</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>port d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HBA</td>
<td>port a</td>
<td></td>
<td></td>
<td>1</td>
<td>30</td>
<td>54</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>port b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA</td>
<td></td>
<td></td>
<td>1</td>
<td>31</td>
<td>55</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>port c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA</td>
<td></td>
<td></td>
<td>2</td>
<td>31</td>
<td>55</td>
<td>19</td>
</tr>
<tr>
<td>Stack 1</td>
<td>bridge_x_51</td>
<td>FC1</td>
<td></td>
<td>1</td>
<td>32</td>
<td>56</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td></td>
<td>2</td>
<td>32</td>
<td>56</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bridge_x_51</td>
<td>FC1</td>
<td>1</td>
<td>33</td>
<td>57</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>FC1</td>
<td>2</td>
<td>33</td>
<td>57</td>
<td>21</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_52</td>
<td>FC1</td>
<td></td>
<td>1</td>
<td>34</td>
<td>58</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td></td>
<td>2</td>
<td>34</td>
<td>58</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bridge_x_52</td>
<td>FC1</td>
<td>1</td>
<td>35</td>
<td>59</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>FC1</td>
<td>2</td>
<td>35</td>
<td>59</td>
<td>23</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_53</td>
<td>FC1</td>
<td></td>
<td>1</td>
<td>36</td>
<td>60</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td></td>
<td>2</td>
<td>36</td>
<td>60</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bridge_x_53</td>
<td>FC1</td>
<td>1</td>
<td>37</td>
<td>61</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>FC1</td>
<td>2</td>
<td>37</td>
<td>61</td>
<td>-</td>
</tr>
<tr>
<td>Stack y</td>
<td>bridge_x_5y</td>
<td>FC1</td>
<td></td>
<td>1</td>
<td>38</td>
<td>62</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td></td>
<td>2</td>
<td>38</td>
<td>62</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bridge_x_5y</td>
<td>FC1</td>
<td>1</td>
<td>39</td>
<td>63</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>FC1</td>
<td>2</td>
<td>39</td>
<td>63</td>
<td>-</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>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>Switch model</td>
<td>ISL port</td>
<td>Switch port</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------</td>
<td>-------------</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>

**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>Cisco 9396S</th>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>FC-VI port b</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>FC-VI port c</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>FC-VI port d</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port a</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port b</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port c</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_1</td>
<td>HBA port d</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>FC-VI port b</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>FC-VI port c</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>FC-VI port d</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>HBA port a</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>HBA port b</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>HBA port c</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>controller_x_2</td>
<td>HBA port d</td>
<td>-</td>
<td>8</td>
</tr>
<tr>
<td>Component</td>
<td>Port</td>
<td>Switch 1</td>
<td>Switch 2</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>----------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>49</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>51</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>52</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>53</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>54</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>55</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>56</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>56</td>
<td></td>
</tr>
</tbody>
</table>

Cisco 9148S

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</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_2</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>
### Cisco 9148S

<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>
</tbody>
</table>

### Cisco 9132T

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</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>
</tbody>
</table>
### Cisco 9132T

#### MDS module 1

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_2</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>

#### MDS module 2

<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>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>
### Cisco 9148 or 9250i*

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</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>HBA port a</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>6</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>
</tbody>
</table>
### Cisco 9396S

<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_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.

### 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_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>
### 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></td>
<td></td>
<td></td>
<td></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>
<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>
</tbody>
</table>
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_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.

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.

<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>bridge_x_8b</td>
<td>FC1</td>
<td>-</td>
</tr>
</tbody>
</table>

Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.
**Cisco 9148S**

<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_1a</td>
<td>FC1</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
<td>9</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_3b</td>
<td>FC1</td>
<td>-</td>
<td>11</td>
</tr>
<tr>
<td>bridge_x_4a</td>
<td>FC1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_4b</td>
<td>FC1</td>
<td>-</td>
<td>12</td>
</tr>
<tr>
<td>bridge_x_5a</td>
<td>FC1</td>
<td>13</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_5b</td>
<td>FC1</td>
<td>-</td>
<td>13</td>
</tr>
<tr>
<td>bridge_x_6a</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_6b</td>
<td>FC1</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_7a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_7b</td>
<td>FC1</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_8a</td>
<td>FC1</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_8b</td>
<td>FC1</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 25 through 48 following the same pattern.

**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_1a</td>
<td>FC1</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_1b</td>
<td>FC1</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td>bridge_x_2b</td>
<td>FC1</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>17</td>
<td>-</td>
</tr>
<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>
</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_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>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>

Cabling the cluster interconnect in eight- or four-node configurations

In eight- or four-node MetroCluster configurations, you must cable the cluster interconnect between the local controller modules at each site.

About this task

This task is not required on two-node MetroCluster configurations.
This task must be performed at both MetroCluster sites.

Step

1. Cable the cluster interconnect from one controller module to the other, or if cluster interconnect switches are used, from each controller module to the switches.

Related information

Network and LIF management

Cabling the cluster peering connections

You must cable the controller module ports used for cluster peering so that they have connectivity with the cluster on the partner site.

About this task

This task must be performed on each controller module in the MetroCluster configuration.

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.

Related concepts

Considerations for configuring cluster peering on page 10

Related information

Cluster and SVM peering express configuration

Cabling the HA interconnect, if necessary

If you have an eight- or a four-node MetroCluster configuration and the storage controllers within the HA pairs are in separate chassis, you must cable the HA interconnect between the controllers.

About this task

• This task does not apply to two-node MetroCluster configurations.

• This task must be performed at both MetroCluster sites.

• The HA interconnect must be cabled only if the storage controllers within the HA pair are in separate chassis.

Some storage controller models support two controllers in a single chassis, in which case they use an internal HA interconnect.
Steps

1. Cable the HA interconnect if the storage controller's HA partner is in a separate chassis.

   AFF and FAS Documentation Center

2. If the MetroCluster site includes two HA pairs, repeat the previous steps on the second HA pair.

3. Repeat this task at the MetroCluster partner site.

Cabling the management and data connections

You must cable the management and data ports on each storage controller to the site networks.

About this task

This task must be repeated for each new controller at both MetroCluster sites.

You can connect the controller and cluster switch management ports to existing switches in your network or to new dedicated network switches such as NetApp CN1601 cluster management switches.

Step

1. Cable the controller's management and data ports to the management and data networks at the local site.

   AFF and FAS Documentation Center

Configuring the FC switches

For fabric-attached MetroCluster systems that were not pre-configured in the factory, you must configure each FC switch in the DR group. This is done manually, or, depending on the switch, can optionally be done with a configuration file.

About this task

For new systems, the FC switch fabrics are typically configured for two ISLs and do not require additional configuration unless you want to change the pre-configured IP addresses.

Choices

- Configuring the FC switches by running a configuration file on page 70
- Configuring the Cisco or Brocade FC switches manually on page 72

Configuring the FC switches by running a configuration file

If you want to simplify the process of configuring switches, you can download and apply switch configuration files that provide the complete switch settings for certain configurations.

About this task

The reference configuration files (RCFs) do not support configurations using eight ISLs. If you are using eight ISLs you must configure the switches manually.

The RCFs apply to two-node, four-node, and eight-node MetroCluster configurations. These files configure the fabric for in-order delivery (IOD) by default.

The RCF download page indicates the number of nodes supported by the different switch models.
Choices

• Configuring Brocade FC switches with configuration files on page 71
• Configuring the Cisco FC switches with RCF files on page 71

Configuring Brocade FC switches with configuration files

When you configure a Brocade FC switch, you can download and apply the switch configuration files that provide the complete switch settings for certain configurations.

Before you begin

You must have access to an FTP server. The switches must have connectivity with the FTP server.

About this task

Each configuration file is different and must be used with the correct switch. Only one of the configuration files for each switch fabric contains zoning commands.

Steps

1. Locate the reference configuration (RCF) files for your configuration.
   You must use the RCF files that match your switch model.
   
   NetApp Downloads: MetroCluster Configuration Files for Brocade Switches

2. Apply the RCF files, following the directions on the Download page and adjusting the ISL settings as needed.

3. 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.
   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.

4. Verify that the ports are online:
   • For Brocade switches, use the switchshow command.
   • For Cisco switches, use the show interface brief command.

5. Cable the FC-VI ports from the controllers to the switches.

6. From the existing nodes, verify that the FC-VI ports are online:
   metrocluster interconnect adapter show
   metrocluster interconnect mirror show

Configuring the Cisco FC switches with RCF files

To configure a Cisco FC switch, you can download and apply the reference configuration (RCF) files that provide the complete switch settings for certain configurations.

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 Cisco Switches

2. Apply the RCF files, following the directions on the Download page and adjusting the inter-switch link (ISL) settings as needed.
3. 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.

   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.

4. Verify that the ports are online:
   • For Brocade switches, use the `switchshow` command.
   • For Cisco switches, use the `show interface brief` command.

5. Cable the FC-VI ports from the controllers to the switches.

6. From the existing nodes, verify that the FC-VI ports are online:
   
   ```
   metrocluster interconnect adapter show
   metrocluster interconnect mirror show
   ```

### Configuring the Cisco or Brocade FC switches manually

Switch configuration procedures and commands are different, depending on the switch vendor.

#### Choices

- Configuring the Brocade FC switches on page 72
- Configuring the Cisco FC switches on page 118

#### Configuring the Brocade FC switches

You must configure each of the Brocade switch fabrics in the MetroCluster configuration.

#### Before you begin

- You must have a PC or UNIX workstation with Telnet or Secure Shell (SSH) access to the FC switches.
- You must be using four supported Brocade switches of the same model with the same Brocade Fabric Operating System (FOS) version and licensing.

    **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.

- The four supported Brocade switches must be connected to two fabrics of two switches each, with each fabric spanning both sites.

- Each storage controller must have four initiator ports available to connect to the switch fabrics. Two initiator ports must be connected from each storage controller to each fabric.

**Note:** You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems with two initiators ports per controller (a single initiator port to each fabric) if all the following criteria are met:

- There are fewer than four FC initiator ports available to connect the disk storage and no additional ports can be configured as FC initiators.
- All slots are in use and no FC initiator card can be added.
About this task

• You should enable Inter-Switch Link (ISL) trunking when it is supported by the links.  
  Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations on page 14

• All ISLs must have the same length and same speed in one fabric.  
  Different lengths can be used in the different fabrics. The same speed must be used in all fabrics.

• Metro-E and TDM (SONET/SDH) are not supported, and any non-FC native framing or signaling is not supported.  
  Metro-E means Ethernet framing or signaling occurs either natively over a Metro distance or through some time-division multiplexing (TDM), multiprotocol label switching (MPLS), or wavelength-division multiplexing (WDM).

• TDMs, FCR (native FC Routing), or FCIP extensions are not supported for the MetroCluster FC switch fabric.

• Certain switches in the MetroCluster FC switch fabric support encryption or compression, and sometimes support both.  
  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.

• The Brocade Virtual Fabric (VF) feature is not supported.

• FC zoning based on domain port is supported, but zoning based on worldwide name (WWN) is not supported.

Steps

1. Reviewing Brocade license requirements on page 73
2. Setting the Brocade FC switch values to factory defaults on page 74
3. Configuring basic switch settings on page 77
4. Configuring basic switch settings on a Brocade DCX 8510-8 switch on page 81
5. Configuring E-ports on Brocade FC switches using FC ports on page 82
6. Configuring 10 Gbps VE ports on Brocade FC 7840 switches on page 88
7. Configuring 40 Gbps VE-ports on Brocade 7840 FC switches on page 90
8. Configuring the non-E-ports on the Brocade switch on page 93
9. Configuring compression on ISL ports a Brocade G620 switch on page 94
10. Configuring zoning on Brocade FC switches on page 95
11. Setting ISL encryption on Brocade 6510 or G620 switches on page 115

Related information
  NetApp Interoperability Matrix Tool

Reviewing Brocade license requirements

You need certain licenses for the switches in a MetroCluster configuration. You must install these licenses on all four switches.

The MetroCluster configuration has the following Brocade license requirements:

• Trunking license for systems using more than one ISL, as recommended.

• Extended Fabric license (for ISL distances over 6 km)
- Enterprise license for sites with more than one ISL and an ISL distance greater than 6 km
  The Enterprise license includes Brocade Network Advisor and all licenses except for additional port licenses.

You can verify that the licenses are installed by using the `licenseshow` command. If you do not have these licenses, you should contact your sales representative before proceeding.

### Setting the Brocade FC switch values to factory defaults

You must set the switch to its factory defaults to ensure a successful configuration. You must also assign each switch a unique name.

**About this task**

In the examples in this procedure, the fabric consists of BrocadeSwitchA and BrocadeSwitchB.

**Steps**

1. Make a console connection and log in to both switches in one fabric.
2. Disable the switch persistently:
   ```
   switchcfgpersistentdisable
   ```
   This ensures the switch will remain disabled after a reboot or fastboot. If this command is not available, use the `switchdisable` command.

**Example**

The following example shows the command on BrocadeSwitchA:

```bash
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

The following example shows the command on BrocadeSwitchB:

```bash
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

3. Enter `switchname switch_name` to set the switch name.
   The switches should each have a unique name. After setting the name, the prompt changes accordingly.

**Example**

The following example shows the command on BrocadeSwitchA:

```bash
BrocadeSwitchA:admin> switchname "FC_switch_A_1"
FC_switch_A_1:admin>
```

The following example shows the command on BrocadeSwitchB:

```bash
BrocadeSwitchB:admin> switchname "FC_Switch_B_1"
FC_switch_B_1:admin>
```

4. Set all ports to their default values by issuing the following command for each port:
   ```
   portcfgdefault
   ```
   This must be done for all ports on the switch.
Example
The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1:admin> portcfgdefault 0
FC_switch_A_1:admin> portcfgdefault 1
...  
FC_switch_A_1:admin> portcfgdefault 39
```

The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1:admin> portcfgdefault 0
FC_switch_B_1:admin> portcfgdefault 1
...  
FC_switch_B_1:admin> portcfgdefault 39
```

5. Clear the zoning information by issuing the following commands:
   - `cfgdisable`
   - `cfgclear`
   - `cfgsave`

Example
The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1:admin> cfgdisable
FC_switch_A_1:admin> cfgclear
FC_switch_A_1:admin> cfgsave
```

The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1:admin> cfgdisable
FC_switch_B_1:admin> cfgclear
FC_switch_B_1:admin> cfgsave
```

6. Set the general switch settings to default:
   - `configdefault`

Example
The following example shows the command on FC_switch_A_1:

```
FC_switch_A_1:admin> configdefault
```

The following example shows the command on FC_switch_B_1:

```
FC_switch_B_1:admin> configdefault
```

7. Set all ports to non-trunking mode:
   - `switchcfgtrunk 0`

Example
The following example shows the command on FC_switch_A_1:

```
FC_switch_A_1:admin> switchcfgtrunk 0
```
The following example shows the command on FC_switch_B_1:

```
FC_switch_B_1:admin> switchcfgtrunk 0
```

8. On Brocade 6510 switches, disable the Brocade Virtual Fabrics (VF) feature:

```
fosconfig options
```

**Example**

The following example shows the command on FC_switch_A_1:

```
FC_switch_A_1:admin> fosconfig --disable vf
```

The following example shows the command on FC_switch_B_1:

```
FC_switch_B_1:admin> fosconfig --disable vf
```

9. Clear the Administrative Domain (AD) configuration:

```
ad options
```

**Example**

The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1:admin> switch:admin> ad --select AD0
FC_switch_A_1:admin> adzone --noaccess
FC_switch_A_1:admin> cfgsave
FC_switch_A_1:admin> exit
FC_switch_A_1:admin> ad --clear -f
FC_switch_A_1:admin> ad --apply
FC_switch_A_1:admin> ad --save
FC_switch_A_1:admin> exit
```

The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1:admin> switch:admin> ad --select AD0
FC_switch_B_1:admin> adzone --noaccess
FC_switch_B_1:admin> cfgsave
FC_switch_B_1:admin> exit
FC_switch_B_1:admin> ad --clear -f
FC_switch_B_1:admin> ad --apply
FC_switch_B_1:admin> ad --save
FC_switch_B_1:admin> exit
```

10. Reboot the switch by issuing the following command:

```
reboot
```

**Example**

The following example shows the command on FC_switch_A_1:

```
FC_switch_A_1:admin> reboot
```

The following example shows the command on FC_switch_B_1:

```
FC_switch_B_1:admin> reboot
```
Configuring basic switch settings

You must configure basic global settings, including the domain ID, for Brocade switches.

About this task

This task contains steps that must be performed on each switch at both of the MetroCluster sites.

In this procedure, you set the unique domain ID for each switch as shown in the following example. In the example, domain IDs 5 and 7 form fabric_1, and domain IDs 6 and 8 form fabric_2.

- FC_switch_A_1 is assigned to domain ID 5
- FC_switch_A_2 is assigned to domain ID 6
- FC_switch_B_1 is assigned to domain ID 7
- FC_switch_B_2 is assigned to domain ID 8

Steps

1. Enter configuration mode:
   ```
   configure
   ```

2. Proceed through the prompts:
   a. Set the domain ID for the switch.
   b. Press Enter in response to the prompts until you get to RDP Polling Cycle, and then set that value to 0 to disable the polling.
   c. Press Enter until you return to the switch prompt.

   Example
   ```
   FC_switch_A_1:admin> configure
   Fabric parameters = y
   Domain_id = 5
   .
   .
   RSCN Transmission Mode [yes, y, no, no: [no] y
   End-device RSCN Transmission Mode
   (0 = RSCN with single PID, 1 = RSCN with multiple PIDS, 2 = Fabric RSCN): (0..2) [1]
   Domain RSCN To End-device for switch IP address or name change
   (0 = disabled, 1 = enabled): (0..1) [0] 1
   .
   RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
   ```

3. If you are using two or more ISLs per fabric, then you can configure either in-order delivery (IOD) of frames or out-of-order (OOD) delivery of frames.

   Note: The standard IOD settings are recommended. You should configure OOD only if necessary.

   Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations on page 14

   - The following steps must be performed on each switch fabric to configure IOD of frames:
     a. Enable IOD:
        ```
        iodset
        ```
b. Set the Advanced Performance Tuning (APT) policy to 1:
   `aptpolicy 1`

c. Disable Dynamic Load Sharing (DLS):
   `dlreset`

d. Verify the IOD settings by using the `iodshow`, `aptpolicy`, and `dlsshow` commands. For example, issue the following commands on FC_switch_A_1:
   ```
   FC_switch_A_1:admin> iodshow
   IOD is set
   FC_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
   
   FC_switch_A_1:admin> dlsshow
   DLS is not set
   ```

e. Repeat these steps on the second switch fabric.

• The following steps must be performed on each switch fabric to configure OOD of frames:

a. Enable OOD:
   `iodreset`

b. Set the Advanced Performance Tuning (APT) policy to 3:
   `aptpolicy 3`

c. Disable Dynamic Load Sharing (DLS):
   `dlreset`

d. Verify the OOD settings by using the `iodshow`, `aptpolicy` and `dlsshow` commands. For example, issue the following commands on FC_switch_A_1:
   ```
   FC_switch_A_1:admin> iodshow
   IOD is not set
   FC_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
   
   FC_switch_A_1:admin> dlsshow
   DLS is set by default with current routing policy
   ```

e. Repeat these steps on the second switch fabric.

**Note:** When configuring ONTAP on the controller modules, OOD must be explicitly configured on each controller module in the MetroCluster configuration.
4. Verify that the switch is using the dynamic port licensing method.
   a. Run the `licensePort --show` command.

   **Example**
   ```
   FC_switch_A_1:admin> licensePort --show
   24 ports are available in this switch
   Full POD license is installed
   Dynamic POD method is in use
   ```

   **Note:** FabOS versions before 8.0 run the following commands as admin and versions 8.0 and later run them as root.

   b. Enable the root user.
   If the root user is already disabled by Brocade, enable the root user as shown in the following example:

   **Example**
   ```
   FC_switch_A_1:admin> userconfig --change root -e yes
   FC_switch_A_1:admin> rootaccess --set consoleonly
   ```

   c. Run the license command: `licensePort --show`

   **Example**
   ```
   FC_switch_A_1:root> licensePort --show
   24 ports are available in this switch
   Full POD license is installed
   Dynamic POD method is in use
   ```

   d. Change the license method to dynamic: `licensePort --method dynamic`

   **Note:** If the dynamic license method is not in use (if the method is static), you must change the license method to dynamic. Skip this step if the dynamic license method is in use.

   **Example**
   ```
   FC_switch_A_1:admin> licensePort --method dynamic
   The POD method has been changed to dynamic.
   Please reboot the switch now for this change to take effect
   ```

5. Enable the trap for T11-FC-ZONE-SERVER-MIB to provide successful health monitoring of the switches in ONTAP:
   a. Enable the T11-FC-ZONE-SERVER-MIB:
      ```
      snmpconfig --set mibCapability -mib_name T11-FC-ZONE-SERVER-MIB -bitmask 0x3f
      ```
   b. Enable the T11-FC-ZONE-SERVER-MIB trap:
      ```
      snmpconfig --enable mibcapability -mib_name SW-MIB -trap_name swZoneConfigChangeTrap
      ```
   c. Repeat the previous steps on the second switch fabric.

6. Optional: If you set the community string to a value other than “public”, you must configure the ONTAP Health Monitors using the community string you specify:
a. Change the existing community string:

```
   snmpconfig --set snmpv1
```

b. Press Enter until you see the Community (ro): [public] text.

c. Enter the desired community string.

**Example**

On FC_switch_A_1:

```bash
FC_switch_A_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
    Community (rw): [Secret C0de]
    Trap Recipient's IP address : [0.0.0.0]
    Community (rw): [OrigEquipMfr]
    Trap Recipient's IP address : [0.0.0.0]
    Community (rw): [private]
    Trap Recipient's IP address : [0.0.0.0]
    Community (ro): [public] mcchm
    change the community string to the desired value, in this example it is set to 'mcchm'
    Community (ro): [common]
    Trap Recipient's IP address : [0.0.0.0]
    Community (ro): [FibreChannel]
    Trap Recipient's IP address : [0.0.0.0]
    Committing configuration....done.
FC_switch_A_1:admin>
```

On FC_switch_B_1:

```bash
FC_switch_B_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
    Community (rw): [Secret C0de]
    Trap Recipient's IP address : [0.0.0.0]
    Community (rw): [OrigEquipMfr]
    Trap Recipient's IP address : [0.0.0.0]
    Community (rw): [private]
    Trap Recipient's IP address : [0.0.0.0]
    Community (ro): [public] mcchm
    change the community string to the desired value, in this example it is set to 'mcchm'
    Community (ro): [common]
    Trap Recipient's IP address : [0.0.0.0]
    Community (ro): [FibreChannel]
    Trap Recipient's IP address : [0.0.0.0]
    Committing configuration....done.
FC_switch_B_1:admin>
```

7. Reboot the switch:

```
reboot
```

**Example**

On FC_switch_A_1:

```bash
FC_switch_A_1:admin> reboot
```

On FC_switch_B_1:

```bash
FC_switch_B_1:admin> reboot
```
8. Persistently enable the switch:

\texttt{switchcfgpersistentenable}

\textbf{Example}

On FC\textunderscore switch\textunderscore A\textunderscore 1:

\begin{verbatim}
FC_switch_A_1:admin> switchcfgpersistentenable
\end{verbatim}

On FC\textunderscore switch\textunderscore B\textunderscore 1:

\begin{verbatim}
FC_switch_B_1:admin> switchcfgpersistentenable
\end{verbatim}

\textbf{Configuring basic switch settings on a Brocade DCX 8510-8 switch}

You must configure basic global settings, including the domain ID, for Brocade switches.

\textbf{About this task}

You must perform the steps on each switch at both MetroCluster sites. In this procedure, you set the domain ID for each switch as shown in the following examples:

- FC\textunderscore switch\textunderscore A\textunderscore 1 is assigned to domain ID 5
- FC\textunderscore switch\textunderscore A\textunderscore 2 is assigned to domain ID 6
- FC\textunderscore switch\textunderscore B\textunderscore 1 is assigned to domain ID 7
- FC\textunderscore switch\textunderscore B\textunderscore 2 is assigned to domain ID 8

In the previous example, domain IDs 5 and 7 form fabric\textunderscore 1, and domain IDs 6 and 8 form fabric\textunderscore 2.

\textbf{Note:} You can also use this procedure to configure the switches when you are only using one DCX 8510-8 switch per site.

Using this procedure, you should create two logical switches on each Brocade DCX 8510-8 switch. The two logical switches created on both Brocade DCX8510-8 switches will form two logical fabrics as shown in the following examples:

- \textbf{LOGICAL FABRIC 1}: Switch1/Blade1 and Switch 2 Blade 1
- \textbf{LOGICAL FABRIC 2}: Switch1/Blade2 and Switch 2 Blade 2

\textbf{Steps}

1. Enter the command mode:

\texttt{configure}

2. Proceed through the prompts:

   a. Set the domain ID for the switch.

   b. Keep selecting \textbf{Enter} until you get to RDP Polling Cycle, and then set the value to 0 to disable the polling.

   c. Select \textbf{Enter} until you return to the switch prompt.
Repeat these steps on all switches in fabric_1 and fabric_2.

4. Configure the virtual fabrics.
   a. Enable virtual fabrics on the switch:
      `fosconfig --enablevf`
   b. Configure the system to use the same base configuration on all logical switches:
      `configurechassis`

Example

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

```
System (yes, y, no, n): [no]  n
cfgload attributes (yes, y, no, n): [no]  n
Custom attributes (yes, y, no, n): [no]  y
Config Index (0 to ignore): (0..1000) [3]:
```

5. Create and configure the logical switch:
   `sconf --create fabricID`

6. Add all ports from a blade to the virtual fabric:
   `lscfg --config fabricID -slot slot -port lowest-port - highest-port`

Example

**Note:** The blades forming a logical fabric (e.g. Switch 1 Blade 1 and Switch 3 Blade 1) need to have the same fabric ID.

```
setcontext fabricid
switchdisable
configure
<configure the switch per the above settings>
switchname unique switch name
switchenable
```

**Related concepts**

*Requirements for using a Brocade DCX 8510-8 switch* on page 15

**Configuring E-ports on Brocade FC switches using FC ports**

For Brocade switches on which the Inter-Switch Links (ISL) are configured using FC ports, you must configure the switch ports on each switch fabric that connect the ISL. These ISL ports are also known as E-ports.

**Before you begin**

- All of the ISLs in an FC switch fabric must be configured with the same speed and distance.
• The combination of the switch port and small form-factor pluggable (SFP) must support the speed.

• The supported ISL distance depends on the FC switch model.

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.

• The ISL link must have a dedicated lambda, and the link must be supported by Brocade for the distance, switch type, and Fabric Operating System (FOS).

About this task

You must not use the L0 setting when issuing the `portCfgLongDistance` command. Instead, you should use the LE or LS setting to configure the distance on the Brocade switches with a minimum of LE distance level.

You must not use the LD setting when issuing the `portCfgLongDistance` command when working with xWDM/TDM equipment. Instead, you should use the LE or LS setting to configure the distance on the Brocade switches.

You must perform this task for each FC switch fabric.

The following tables show the ISL ports for different switches and different number of ISLs in a configuration running ONTAP 9.1 or 9.2. The examples shown in this section are for a Brocade 6505 switch. You should modify the examples to use ports that apply to your switch type.

If your configuration is running ONTAP 9.0 or earlier, see the “Port assignments for FC switches when using ONTAP 9.0” section in the Fabric-attached MetroCluster Installation and Configuration Guide.

You must use the required number of ISLs for your configuration.

<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>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>
</tbody>
</table>
### Switch model

<table>
<thead>
<tr>
<th>ISL port</th>
<th>Switch port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade 7840</td>
<td>ISL port 1 ge0 (40-Gbps) or ge2 (10-Gbps)</td>
</tr>
<tr>
<td></td>
<td>ISL port 2 ge1 (40-Gbps) or ge3 (10-Gbps)</td>
</tr>
<tr>
<td></td>
<td>ISL port 3 ge10 (10-Gbps)</td>
</tr>
<tr>
<td></td>
<td>ISL port 4 ge11 (10-Gbps)</td>
</tr>
<tr>
<td>Brocade G10</td>
<td>ISL port 1 20</td>
</tr>
<tr>
<td></td>
<td>ISL port 2 21</td>
</tr>
<tr>
<td></td>
<td>ISL port 3 22</td>
</tr>
<tr>
<td></td>
<td>ISL port 4 23</td>
</tr>
<tr>
<td>Brocade G620 and Brocade G630</td>
<td>ISL port 1 40</td>
</tr>
<tr>
<td></td>
<td>ISL port 2 41</td>
</tr>
<tr>
<td></td>
<td>ISL port 3 42</td>
</tr>
<tr>
<td></td>
<td>ISL port 4 43</td>
</tr>
<tr>
<td></td>
<td>ISL port 5 44</td>
</tr>
<tr>
<td></td>
<td>ISL port 6 45</td>
</tr>
<tr>
<td></td>
<td>ISL port 7 46</td>
</tr>
<tr>
<td></td>
<td>ISL port 8 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.

### Steps

1. Configure the port speed:

   ```
   portcfgspeed port-number speed
   ```

   You must use the highest common speed that is supported by the components in the path.

   **Example**

   In the following example, there are two ISLs for each fabric:

   ```
   FC_switch_A_1:admin> portcfgspeed 20 16
   FC_switch_A_1:admin> portcfgspeed 21 16
   FC_switch_B_1:admin> portcfgspeed 20 16
   FC_switch_B_1:admin> portcfgspeed 21 16
   ```

2. Configure the trunking mode for each ISL:

   ```
   portcfgtrunkport port-number
   ```

   - If you are configuring the ISLs for trunking (IOD), set the `portcfgtrunkport port-number` to 1 as shown in the following example:

   ```
   FC_switch_A_1:admin> portcfgtrunkport 20 1
   FC_switch_A_1:admin> portcfgtrunkport 21 1
   FC_switch_B_1:admin> portcfgtrunkport 20 1
   FC_switch_B_1:admin> portcfgtrunkport 21 1
   ```
If you do not want to configure the ISL for trunking (OOD), set `portcfgtrunk port-number` to 0 as shown in the following example:

```
FC_switch_A_1:admin> portcfgtrunkport 20 0
FC_switch_A_1:admin> portcfgtrunkport 21 0
FC_switch_B_1:admin> portcfgtrunkport 20 0
FC_switch_B_1:admin> portcfgtrunkport 21 0
```

3. Enable QoS traffic for each of the ISL ports:

```
portcfgqos --enable port-number
```

**Example**

In the following example, there are two ISLs per switch fabric:

```
FC_switch_A_1:admin> portcfgqos --enable 20
FC_switch_A_1:admin> portcfgqos --enable 21
FC_switch_B_1:admin> portcfgqos --enable 20
FC_switch_B_1:admin> portcfgqos --enable 21
```

4. Verify the settings:

```
portCfgShow command
```

**Example**

The following example shows the output for a configuration that uses two ISLs cabled to port 20 and port 21. The Trunk Port setting should be **ON** for IOD and **OFF** for OOD:

```
<table>
<thead>
<tr>
<th>Ports of Slot 0</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>8G</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>16G</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
<td>AN</td>
</tr>
<tr>
<td>Fill Word</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AL_PA Offset</td>
<td>13</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Trunk Port</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
</tr>
<tr>
<td>Long Distance</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>VC Link Init</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Locked L_Port</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Locked E_Port</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Disabled E_Port</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>ISL R_RDY Mode</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>RSCN Suppressed</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Persistent Disable</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>LOS TOL enable</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>NPIV capability</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
</tr>
<tr>
<td>NPIV PP Limit</td>
<td>126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mirror Port</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Rate Limit</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Credit Recovery</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
</tr>
<tr>
<td>FPort Buffers</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Port Auto Disable</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>CSCTL mode</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Fault Delay</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

5. Calculate the ISL distance.

Because of the behavior of FC-VI, the distance must be set to 1.5 times the real distance with a minimum distance of 10 km (using the LE distance level).

The distance for the ISL is calculated as follows, rounded up to the next full kilometer:

\[
1.5 \times \text{real\_distance} = \text{distance}
\]
Example

If the distance is 3 km, then $1.5 \times 3 \text{ km} = 4.5 \text{ km}$. This is lower than 10 km, so the ISL must be set to the LE distance level.

If the distance is 20 km, then $1.5 \times 20 \text{ km} = 30 \text{ km}$. The ISL must be set to 30 km and must use the LS distance level.

6. Set the distance on each ISL port:

```
porthdistance longdistance
```

`portdistance` level `vc_link_init distance`

A `vc_link_init` value of 1 uses the ARB fill word (default). A value of 0 uses IDLE. The required value might depend on the link being used. The commands must be repeated for each ISL port.

Example

For an ISL distance of 3 km, as given in the example in the previous step, the setting is 4.5 km with the default `vc_link_init` value of 1. Because a setting of 4.5 km is lower than 10 km, the port needs to be set to the LE distance level:

```
FC_switch_A_1:admin> portcfglongdistance 20 LE 1
FC_switch_B_1:admin> portcfglongdistance 20 LE 1
```

For an ISL distance of 20 km, as given in the example in the previous step, the setting is 30 km with the default `vc_link_init` value of 1:

```
FC_switch_A_1:admin> portcfglongdistance 20 LS 1 -distance 30
FC_switch_B_1:admin> portcfglongdistance 20 LS 1 -distance 30
```

7. Verify the distance setting:

```
porthbuffershow
```

A distance level of LE appears as 10 km.

Example

The following example shows the output for a configuration that uses ISLs on port 20 and port 21:

```
FC_switch_A_1:admin> porthbuffershow

<table>
<thead>
<tr>
<th>User Port</th>
<th>Port Type</th>
<th>Lx Mode</th>
<th>Max/Resv Buffers</th>
<th>Buffer Needed Usage Buffers</th>
<th>Link Distance Buffers</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>20 E</td>
<td>-</td>
<td>8</td>
<td>67</td>
<td>67</td>
<td>30km</td>
</tr>
<tr>
<td>21 E</td>
<td>-</td>
<td>8</td>
<td>67</td>
<td>67</td>
<td>30km</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>23</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
<td>466</td>
</tr>
</tbody>
</table>
```

8. Verify that both switches form one fabric:

```
switchshow
```

Example

The following example shows the output for a configuration that uses ISLs on port 20 and port 21:
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 5
switchId: fffc01
switchWwn: 10:00:00:05:33:86:89:cb
zoning: OFF
switchBeacon: OFF

Index Port Address Media Speed State Proto
-------------------------------------------
...
20   20  010C00   id    16G  Online FC  LE E-Port  10:00:00:05:33:8c:2e:9a
"FC_switch_B_1" (downstream)(trunk master)
21   21  010D00   id    16G  Online FC  LE E-Port  (Trunk port, master is Port 20)
...

FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchState: Online
switchMode: Native
switchRole: Principal
switchDomain: 7
switchId: fffc03
switchWwn: 10:00:00:05:33:8c:2e:9a
zoning: OFF
switchBeacon: OFF

Index Port Address Media Speed State Proto
-------------------------------------------
...
20   20  030C00   id    16G  Online FC  LE E-Port  10:00:00:05:33:86:89:cb
"FC_switch_B_1" (downstream)(Trunk master)
21   21  030D00   id    16G  Online FC  LE E-Port  (Trunk port, master is Port 20)
...

9. Confirm the configuration of the fabrics:

   fabricshow

Example

FC_switch_A_1:admin> fabricshow
Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:8c:2e:9a 10.10.10.55 0.0.0.0 "FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65 0.0.0.0 "FC_switch_B_1"

FC_switch_B_1:admin> fabricshow
Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:8c:2e:9a 10.10.10.55 0.0.0.0 "FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65 0.0.0.0 "FC_switch_B_1"

10. Confirm the trunking of the ISLs:

   trunkshow

   • If you are configuring the ISLs for trunking (IOD), you should see output similar to the following:

   FC_switch_A_1:admin> trunkshow
   1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
      21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16
   FC_switch_B_1:admin> trunkshow
If you are not configuring the ISLs for trunking (OOD), you should see output similar to the following:

FC_switch_A_1:admin> trunkshow
1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
2: 21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16 MASTER

FC_switch_B_1:admin> trunkshow
1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
2: 21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16 MASTER

11. Repeat Step 1 on page 84 through Step 10 on page 87 for the second FC switch fabric.

Related concepts
Port assignments for FC switches when using ONTAP 9.1 and later on page 52

Configuring 10 Gbps VE ports on Brocade FC 7840 switches

When using the 10 Gbps VE ports (which use FCIP) for ISLs, you must create IP interfaces on each port, and configure FCIP tunnels and circuits in each tunnel.

About this task
This procedure must be performed on each switch fabric in the MetroCluster configuration.

The examples in this procedure assume that the two Brocade 7840 switches have the following IP addresses:

- FC_switch_A_1 is local.
- FC_switch_B_1 is remote.

Steps

1. Create IP interface (ipif) addresses for the 10 Gbps ports on both switches in the fabric:

   portcfg ipif FC_switch1_name first_port_name create
   FC_switch1_IP_address netmask netmask_number vlan 2 mtu auto

Example

The following command creates ipif addresses on ports ge2.dp0 and ge3.dp0 of FC_switch_A_1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>portcfg ipif ge2.dp0 create</td>
<td>10.10.20.71 netmask 255.255.0.0 vlan 2</td>
</tr>
<tr>
<td>portcfg ipif ge3.dp0 create</td>
<td>10.10.21.71 netmask 255.255.0.0 vlan 2</td>
</tr>
</tbody>
</table>

Example

The following command creates ipif addresses on ports ge2.dp0 and ge3.dp0 of FC_switch_B_1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>portcfg ipif ge2.dp0 create</td>
<td>10.10.20.72 netmask 255.255.0.0 vlan 2</td>
</tr>
<tr>
<td>portcfg ipif ge3.dp0 create</td>
<td>10.10.21.72 netmask 255.255.0.0 vlan 2</td>
</tr>
</tbody>
</table>

2. Verify that the ipif addresses were created successfully on both switches:
portshow ipif all

Example
The following command shows the ipif addresses on switch FC_switch_A_1:

```
FC_switch_A_1:root> portshow ipif all
Port         IP Address                     / Pfx  MTU   VLAN  Flags
---------------------------------------------------------------
ge2.dp0      10.10.20.71                    / 24   AUTO  2     U R M I
ge3.dp0      10.10.21.71                    / 20   AUTO  2     U R M I
ge10.dp1     10.10.71.10                    / 16   AUTO  2     U R M I
ge11.dp1     10.10.71.11                    / 16   AUTO  2     U R M
```

Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running I=InUse
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport

The following command shows the ipif addresses on switch FC_switch_B_1:

```
FC_switch_B_1:root> portshow ipif all
Port         IP Address                     / Pfx  MTU   VLAN  Flags
---------------------------------------------------------------
ge2.dp0      10.10.20.72                    / 24   AUTO  2     U R M I
ge3.dp0      10.10.21.72                    / 20   AUTO  2     U R M I
ge10.dp1     10.10.72.10                    / 16   AUTO  2     U R M I
ge11.dp1     10.10.72.11                    / 16   AUTO  2     U R M
```

3. Create the first of the two FCIP tunnels using the ports on dp0:

```
portcfg fc iptunnel
```

This command creates a tunnel with a single circuit.

Example
The following command creates the tunnel on switch FC_switch_A_1:

```
portcfg fc iptunnel 24 create -S 10.10.20.71 -D 10.10.20.72 -b 10000000 -B 10000000
```

The following command creates the tunnel on switch FC_switch_B_1:

```
portcfg fc iptunnel 24 create -S 10.10.20.72 -D 10.10.20.71 -b 10000000 -B 10000000
```

4. Create the second of the two FCIP tunnels using the ports on dp1:

```
portcfg fc iptunnel
```

Example
The following command creates the tunnel on switch FC_switch_A_1:

```
portcfg fc iptunnel 35 create -S 10.10.71.10 -D 10.10.72.10 -b 10000000 -B 10000000
```

The following command creates the tunnel on switch FC_switch_B_1:

```
portcfg fc iptunnel 35 create -S 10.10.72.10 -D 10.10.71.10 -b 10000000 -B 10000000
```

5. Verify that the FCIP tunnels were successfully created:

```
portshow fc iptunnel all
```

Example
The following example shows that the tunnels were created and the circuits are up:
6. Create an additional circuit for dp0 and dp1.

Example

The following command creates a circuit on switch FC_switch_A_1 for dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.71 -D 10.10.21.72 --min-comm-rate 5000000 --max-comm-rate 5000000
```

The following command creates a circuit on switch FC_switch_B_1 for dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.72 -D 10.10.21.71 --min-comm-rate 5000000 --max-comm-rate 5000000
```

The following command creates a circuit on switch FC_switch_A_1 for dp1:

```
portcfg fcipcircuit 35 create 3 -S 10.10.71.11 -D 10.10.72.11 --min-comm-rate 5000000 --max-comm-rate 5000000
```

The following command creates a circuit on switch FC_switch_B_1 for dp1:

```
portcfg fcipcircuit 35 create 1 -S 10.10.72.11 -D 10.10.71.11 --min-comm-rate 5000000 --max-comm-rate 5000000
```

7. Verify that all circuits were successfully created:

```
portshow fcipcircuit all
```

Example

The following command shows the circuits and their status:

```
FC_switch_A_1:root> portshow fcipcircuit all
```

---

**Configuring 40 Gbps VE-ports on Brocade 7840 FC switches**

When using the two 40 GbE VE-ports (which use FCIP) for ISLs, you must create IP interfaces on each port, and configure FCIP tunnels and circuits in each tunnel.

**About this task**

This procedure must be performed on each switch fabric in the MetroCluster configuration.

The examples in this procedure use two switches:

- FC_switch_A_1 is local.
Steps

1. Create IP interface (ipif) addresses for the 40 Gbps ports on both switches in the fabric:

   ```
   portcfg ipif FC_switch_name first_port_name create FC_switch_IP_address netmask netmask_number vlan 2 mtu auto
   ```

   **Example**

   The following command creates ipif addresses on ports ge0.dp0 and ge1.dp0 of FC_switch_A_1:

   ```
   portcfg ipif ge0.dp0 create 10.10.82.10 netmask 255.255.0.0 vlan 2 mtu auto
   portcfg ipif ge1.dp0 create 10.10.82.11 netmask 255.255.0.0 vlan 2 mtu auto
   ```

   **Example**

   The following command creates ipif addresses on ports ge0.dp0 and ge1.dp0 of FC_switch_B_1:

   ```
   portcfg ipif ge0.dp0 create 10.10.83.10 netmask 255.255.0.0 vlan 2 mtu auto
   portcfg ipif ge1.dp0 create 10.10.83.11 netmask 255.255.0.0 vlan 2 mtu auto
   ```

2. Verify that the ipif addresses were successfully created on both switches:

   ```
   portshow ipif all
   ```

   **Example**

   The following example shows the IP interfaces on FC_switch_A_1:

   ```
   Port         IP Address                     / Pfx  MTU   VLAN  Flags
   ---------------------------------------------------------------
   ge0.dp0      10.10.82.10                    / 16   AUTO  2     U R M
   ge1.dp0      10.10.82.11                    / 16   AUTO  2     U R M
   ---------------------------------------------------------------
   Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running I=InUse
          N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
   ```

   The following example shows the IP interfaces on FC_switch_B_1:

   ```
   Port         IP Address                     / Pfx  MTU   VLAN  Flags
   ---------------------------------------------------------------
   ge0.dp0      10.10.83.10                    / 16   AUTO  2     U R M
   ge1.dp0      10.10.83.11                    / 16   AUTO  2     U R M
   ---------------------------------------------------------------
   Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running I=InUse
          N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
   ```

3. Create the FCIP tunnel on both switches:

   ```
   portcfig fc iptunnel
   ```

   **Example**

   The following command creates the tunnel on FC_switch_A_1:

   ```
   portcfg fc iptunnel 24 create -S 10.10.82.10 -D 10.10.83.10 -b 100000000
   ```
The following command creates the tunnel on FC_switch_B_1:

```
portcfg fciptunnel 24 create -S 10.10.83.10 -D 10.10.82.10 -b 10000000 -B 10000000
```

4. Verify that the FCIP tunnel has been successfully created:

   `portsshow fciptunnel all`

   **Example**

   The following example shows that the tunnel was created and the circuits are up:

   ```
   Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt CommRt Met/G
   24    -         Up      ---------     2d8m    0.05    0.41   3      -       -
   Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON r=ReservedBW
   a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
   I=IP-Ext
   ```

5. Create an additional circuit on each switch:

   `portcfg fcipcircuit 24 create 1 -S source-IP-address -D destination-IP-address --min-comm-rate 10000000 --max-comm-rate 10000000`

   **Example**

   The following command creates a circuit on switch FC_switch_A_1 for dp0:

   ```
   portcfg fcipcircuit 24 create 1 -S 10.10.82.11 -D 10.10.83.11 --min-comm-rate 10000000 --max-comm-rate 10000000
   ```

   The following command creates a circuit on switch FC_switch_B_1 for dp1:

   ```
   portcfg fcipcircuit 24 create 1 -S 10.10.83.11 -D 10.10.82.11 --min-comm-rate 10000000 --max-comm-rate 10000000
   ```

6. Verify that all circuits were successfully created:

   `portsshow fcipcircuit all`

   **Example**

   The following example lists the circuits and shows that their OpStatus is up:

   ```
   Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt CommRt Met/G
   24    0 ge0     Up      ---va---4    2d12m    0.02    0.03   3 10000/10000 0/-
   24    1 ge1     Up      ---va---4    2d12m    0.02    0.04   3 10000/10000 0/-
   Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4 6=IPv6
   ARL a=Auto r=Reset s=StepDown t=TimedStepDown S=SLA
   ```
Configuring the non-E-ports on the Brocade switch

You must configure the non-E-ports on the FC switch. In a MetroCluster configuration, these are the ports that connect the switch to the HBA initiators, FC-VI interconnects, and FC-to-SAS bridges. These steps must be done for each port.

About this task

In the following example, the ports connect an FC-to-SAS bridge:

- Port 6 on FC_FC_switch_A_1 at Site_A
- Port 6 on FC_FC_switch_B_1 at Site_B

Steps

1. Configure the port speed for each non-E-port:

   \texttt{portcfgspeed \textit{port} \textit{speed}}

   You should use the highest common speed, which is the highest speed supported by all components in the data path: the SFP, the switch port that the SFP is installed on, and the connected device (HBA, bridge, and so on).

   For example, the components might have the following supported speeds:

   - The SFP is capable of 4, 8, or 16 GB.
   - The switch port is capable of 4, 8, or 16 GB.
   - The connected HBA maximum speed is 16 GB.

   The highest common speed in this case is 16 GB, so the port should be configured for a speed of 16 GB.

   \textbf{Example}

   \begin{verbatim}
   FC_switch_A_1:admin> portcfgspeed 6 16
   FC_switch_B_1:admin> portcfgspeed 6 16
   \end{verbatim}

2. Verify the settings:

   \texttt{portcfgshow}

   \textbf{Example}

   \begin{verbatim}
   FC_switch_A_1:admin> portcfgshow
   FC_switch_B_1:admin> portcfgshow
   \end{verbatim}

   In the example output, port 6 has the following settings; speed is set to 16G:

   \begin{verbatim}
<table>
<thead>
<tr>
<th>Ports of Slot 0</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL_PA Offset 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trunk Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long Distance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VC Link Init</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locked L_Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locked G_Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disabled E_Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locked E_Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISL R_RDY Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSCN Suppressed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
   \end{verbatim}
### Configuring compression on ISL ports a Brocade G620 switch

If you are using Brocade G620 switches and enabling compression on the ISLs, you must configure it on each E-port on the switches.

**About this task**

This task must be performed on the ISL ports on both switches using the ISL.

**Steps**

1. Disable the port on which you want to configure compression:
   
   ```
   portdisable port-id
   ```

2. Enable compression on the port:

   ```
   portcfgcompress --enable port-id
   ```

3. Enable the port to activate the configuration with compression:

   ```
   portenable port-id
   ```

4. Confirm that the setting has been changed:

   ```
   portcfgshow port-id
   ```

The following example enables compression on port 0.

```text
FC_switch_A_1:admin> portdisable 0
FC_switch_A_1:admin> portcfgcompress --enable 0
FC_switch_A_1:admin> portenable 0
FC_switch_A_1:admin> portcfgshow 0
Area Number: 0
Octet Speed Combo: 3(16G,10G)
(output truncated)
D-Port mode: OFF
D-Port over DWDM ..
Compression: ON
Encryption: ON
```

You can use the `islShow` command to check that the E_port has come online with encryption or compression configured and active.

```text
FC_switch_A_1:admin> islshow
1: 0-> 0 10:00:c4:f5:7c:8b:29:86  5 FC_switch_B_1
sp: 16.000G bw: 16.000G TRUNK QOS CR_RECOV ENCRYPTION COMPRESSION
```

You can use the `portEncCompShow` command to see which ports are active. In this example you can see that encryption and compression are configured and active on port 0.
Configuring zoning on Brocade FC switches

You must assign the switch ports to separate zones to separate controller and storage traffic. The procedure differs depending on whether you are using a FibreBridge 7500N or FibreBridge 6500N bridge.

Choices

• Zoning for FC-VI ports on page 95
• Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using one FC port on page 98
• Zoning for FibreBridge 7500N bridges using both FC ports on page 104
• Configuring zoning on Brocade FC switches on page 113

Zoning for FC-VI ports

For each DR group in the MetroCluster, you must configure two zones for the FC-VI connections that allow controller-to-controller traffic. These zones contain the FC switch ports connecting to the controller module FC-VI ports. These zones are Quality of Service (QoS) zones.

A QoS zone name starts with the prefix QOSHid_, followed by a user-defined string to differentiate it from a regular zone. These QoS zones are the same regardless of the model of FibreBridge bridge that is being used.

Each zone contains all the FC-VI ports, one for each FC-VI cable from each controller. These zones are configured for high priority.

The following tables show the FC-VI zones for two DR groups.

<table>
<thead>
<tr>
<th>DR group 1: QOSH1 FC-VI zone for FC-VI port a / c</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FC switch</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>FC Switch_A_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Cabling a fabric-attached MetroCluster configuration | 95
### DR group 1: QOSH1 FC-VI zone for FC-VI port a / c

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Switch port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6505 / 6510</td>
<td>6520</td>
<td>G620</td>
</tr>
<tr>
<td><strong>FC_switch_B_1</strong></td>
<td>B</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>controller_B_1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>port FC-VI a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>controller_B_1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>port FC-VI c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>controller_B_2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>port FC-VI a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>controller_B_2</td>
</tr>
</tbody>
</table>

**Zone in Fabric_1**

**Member ports**

QOSH1_MC1_FAB_1_FCVI

5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5

### DR group 1: QOSH1 FC-VI zone for FC-VI port b / d

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Switch port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6505 / 6510</td>
<td>6520</td>
<td>G620</td>
</tr>
<tr>
<td><strong>FC_switch_A_2</strong></td>
<td>A</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>controller_A_1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>port FC-VI b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>controller_A_1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>port FC-VI d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>controller_A_2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>port FC-VI b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>controller_A_2</td>
</tr>
</tbody>
</table>

**Zone in Fabric_1**

**Member ports**

QOSH1_MC1_FAB_2_FCVI

6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5
### DR group 2: QOSH2 FC-VI zone for FC-VI port a / c

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6510</td>
<td>6520</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29</td>
<td>53</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29</td>
<td>53</td>
</tr>
</tbody>
</table>

### Zone in Fabric 1

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>QOSH2_MC2_FAB_1_FCVI (6510)</td>
</tr>
<tr>
<td>5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29</td>
</tr>
<tr>
<td>QOSH2_MC2_FAB_1_FCVI (6520)</td>
</tr>
<tr>
<td>5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53</td>
</tr>
</tbody>
</table>

### DR group 2: QOSH2 FC-VI zone for FC-VI port b / d

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6510</td>
<td>6520</td>
</tr>
<tr>
<td>FC_switch_A_2</td>
<td>A</td>
<td>6</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29</td>
<td>53</td>
</tr>
<tr>
<td>FC_switch_B_2</td>
<td>B</td>
<td>8</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29</td>
<td>53</td>
</tr>
</tbody>
</table>
The following table provides a summary of the FC-VI zones:

<table>
<thead>
<tr>
<th>Fabric</th>
<th>Zone name</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1 and FC_switch_B_1</td>
<td>QOSH1_MC1_FAB_1_FCVI (6510)</td>
<td>5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5</td>
</tr>
<tr>
<td></td>
<td>QOSH2_MC1_FAB_1_FCVI (6510)</td>
<td>5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29</td>
</tr>
<tr>
<td></td>
<td>QOSH2_MC1_FAB_1_FCVI (6520)</td>
<td>5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53</td>
</tr>
<tr>
<td>FC_switch_A_2 and FC_switch_B_2</td>
<td>QOSH1_MC1_FAB_2_FCVI (6510)</td>
<td>6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5</td>
</tr>
<tr>
<td></td>
<td>QOSH2_MC1_FAB_2_FCVI (6510)</td>
<td>6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29</td>
</tr>
<tr>
<td></td>
<td>QOSH2_MC1_FAB_2_FCVI (6520)</td>
<td>6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53</td>
</tr>
</tbody>
</table>

**Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using one FC port**

If you are using FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using only one of the two FC ports, you need to create storage zones for the bridge ports. You should understand the zones and associated ports before you configure the zones.

The examples show zoning for DR group 1 only. If your configuration includes a second DR group, configure the zoning for the second DR group in the same manner, using the corresponding ports of the controllers and bridges.

**Required zones**

You must configure one zone for each of the FC-to-SAS bridge FC ports that allows traffic between initiators on each controller module and that FC-to-SAS bridge.

Each storage zone contains nine ports:

- Eight HBA initiator ports (two connections for each controller)
- One port connecting to an FC-to-SAS bridge FC port

The storage zones use standard zoning.

The examples show two pairs of bridges connecting two stack groups at each site. Because each bridge uses one FC port, there are a total of four storage zones per fabric (eight in total).

**Bridge naming**

The bridges use the following example naming: `bridge_site_stack group location in pair`

<table>
<thead>
<tr>
<th>This portion of the name...</th>
<th>Identifies the...</th>
<th>Possible values...</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>site</code></td>
<td>Site on which the bridge pair physically resides.</td>
<td>A or B</td>
</tr>
</tbody>
</table>
### This portion of the name...  
**Identifies the...**  
**Possible values...**

<table>
<thead>
<tr>
<th>stack group</th>
<th>Number of the stack group to which the bridge pair connects.</th>
<th>1, 2, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• FibreBridge 7600N or 7500N bridges support up to four stacks in the stack group. The stack group can contain no more than 10 storage shelves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FibreBridge 6500N bridges support only a single stack in the stack group.</td>
<td></td>
</tr>
</tbody>
</table>

| location in pair | Bridge within the bridge pair. A pair of bridges connect to a specific stack group. | a or b |

Example bridge names for one stack group on each site:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

#### DR Group 1 - Stack 1 at Site_A

<table>
<thead>
<tr>
<th>DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FC switch</strong></td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>FC_switch_B_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone in Fabric_1</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1</td>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8</td>
</tr>
</tbody>
</table>
### DR Group 1 - Stack 2 at Site_A

#### DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>bridge_A_1b FC1</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>2</td>
<td>controller_B_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0d</td>
</tr>
</tbody>
</table>

#### Zone in Fabric_2

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8</td>
</tr>
</tbody>
</table>

### Zone in Fabric_1

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9</td>
</tr>
</tbody>
</table>

#### DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>2</td>
<td>controller_A_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9</td>
<td>bridge_A_2a FC1</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>2</td>
<td>controller_B_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0c</td>
</tr>
</tbody>
</table>
### DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1

<table>
<thead>
<tr>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td>3</td>
<td>controller_A_1 port 0d</td>
</tr>
<tr>
<td>6</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td>7</td>
<td>controller_A_2 port 0d</td>
</tr>
<tr>
<td>9</td>
<td>bridge_A_2b FC1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>6</td>
<td>2</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0d</td>
</tr>
<tr>
<td>B</td>
<td>8</td>
<td>2</td>
<td>controller_B_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0d</td>
</tr>
</tbody>
</table>

### Zone in Fabric_2

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9</td>
</tr>
</tbody>
</table>

### DR Group 1 - Stack 1 at Site_B

### DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1

<table>
<thead>
<tr>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>controller_A_1 port 0a</td>
</tr>
<tr>
<td>3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td>6</td>
<td>controller_A_2 port 0a</td>
</tr>
<tr>
<td>7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td>2</td>
<td>controller_B_1 port 0a</td>
</tr>
<tr>
<td>3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td>6</td>
<td>controller_B_2 port 0a</td>
</tr>
<tr>
<td>7</td>
<td>controller_B_2 port 0c</td>
</tr>
<tr>
<td>8</td>
<td>bridge_B_1a FC1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>5</td>
<td>2</td>
<td>controller_A_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td>B</td>
<td>7</td>
<td>2</td>
<td>controller_B_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8</td>
<td>bridge_B_1a FC1</td>
</tr>
</tbody>
</table>

### Zone in Fabric_1

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8</td>
</tr>
</tbody>
</table>
### DrGroup 1: MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0d</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>2</td>
<td>controller_B_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>bridge_B_1b FC1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone in Fabric_2</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1</td>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;8,8</td>
</tr>
</tbody>
</table>

### DR Group 1 - Stack 2 at Site_B

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>2</td>
<td>controller_A_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>2</td>
<td>controller_B_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9</td>
<td>bridge_B_2a FC1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone in Fabric_1</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TO_P_FC1</td>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9</td>
</tr>
</tbody>
</table>
## DrGroup 1 : MCI_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_A_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0d</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>2</td>
<td>controller_B_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>controller_B_1 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_B_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_B_2 port 0d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9</td>
<td>bridge_B_1b FC1</td>
</tr>
</tbody>
</table>

### Zone in Fabric_2

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9</td>
</tr>
</tbody>
</table>

### Summary of storage zones

<table>
<thead>
<tr>
<th>Fabric</th>
<th>Zone name</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1 and FC_switch_B_1</td>
<td>MCI_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1</td>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8</td>
</tr>
<tr>
<td></td>
<td>MCI_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1</td>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9</td>
</tr>
<tr>
<td></td>
<td>MCI_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1</td>
<td>5,2;5,3;5,5,6;5,7;7,2;7,3;7,6;7;7,8</td>
</tr>
<tr>
<td></td>
<td>MCI_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1</td>
<td>5,2;5,3;5,6;5,7;7,2;7,3;7,6;7;7,9</td>
</tr>
<tr>
<td>FC_switch_A_2 and FC_switch_B_2</td>
<td>MCI_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1</td>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8</td>
</tr>
<tr>
<td></td>
<td>MCI_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1</td>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9</td>
</tr>
<tr>
<td></td>
<td>MCI_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1</td>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,8</td>
</tr>
<tr>
<td></td>
<td>MCI_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1</td>
<td>6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9</td>
</tr>
</tbody>
</table>
Zoning for FibreBridge 7500N bridges using both FC ports

If you are using FibreBridge 7500N bridges with both FC ports, you need to create storage zones for the bridge ports. You should understand the zones and associated ports before you configure the zones.

Required zones

You must configure one zone for each of the FC-to-SAS bridge FC ports that allows traffic between initiators on each controller module and that FC-to-SAS bridge.

Each storage zone contains five ports:

• Four HBA initiator ports (one connection for each controller)
• One port connecting to an FC-to-SAS bridge FC port

The storage zones use standard zoning.

The examples show two pairs of bridges connecting two stack groups at each site. Because each bridge uses one FC port, there are a total of eight storage zones per fabric (sixteen in total).

Bridge naming

The bridges use the following example naming: bridge_site_stack grouplocation in pair

<table>
<thead>
<tr>
<th>This portion of the name...</th>
<th>Identifies the...</th>
<th>Possible values...</th>
</tr>
</thead>
<tbody>
<tr>
<td>site</td>
<td>Site on which the bridge pair physically resides.</td>
<td>A or B</td>
</tr>
<tr>
<td>stack group</td>
<td>Number of the stack group to which the bridge pair connects.</td>
<td>1, 2, etc.</td>
</tr>
<tr>
<td></td>
<td>• FibreBridge 7600N or 7500N bridges support up to four stacks in the stack group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The stack group can contain no more than 10 storage shelves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FibreBridge 6500N bridges support only a single stack in the stack group.</td>
<td></td>
</tr>
<tr>
<td>location in pair</td>
<td>Bridge within the bridge pair. A pair of bridges connect to a specific stack group.</td>
<td>a or b</td>
</tr>
</tbody>
</table>

Example bridge names for one stack group on each site:

• bridge_A_1a
• bridge_A_1b
• bridge_B_1a
• bridge_B_1b
### DR Group 1 - Stack 1 at Site_A

**DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1**

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_ A_1</td>
<td>A</td>
<td>5</td>
<td>2 2</td>
<td>controller_A_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 6</td>
<td>controller_A_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8 8</td>
<td>bridge_A_1a FC1</td>
</tr>
<tr>
<td>FC_switch_ B_1</td>
<td>B</td>
<td>7</td>
<td>2 2</td>
<td>controller_B_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 6</td>
<td>controller_B_2 port 0a</td>
</tr>
</tbody>
</table>

**Zone in Fabric_1**

| Member ports | 5,2;5,6;7,2;7,6;5,8 |

**DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1**

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_ A_1</td>
<td>A</td>
<td>5</td>
<td>3 3 3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7 7 7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9 9 9</td>
<td>bridge_A_1b FC1</td>
</tr>
<tr>
<td>FC_switch_ B_1</td>
<td>B</td>
<td>7</td>
<td>3 3 3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7 7 7</td>
<td>controller_B_2 port 0c</td>
</tr>
</tbody>
</table>

**Zone in Fabric_2**

| Member ports | 5,3;5,7;7,3;7,7;5,9 |

---

Cabling a fabric-attached MetroCluster configuration | 105
### DrGroup 1: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6505 / 6510 / G610</td>
<td>6520</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

**Zone in Fabric_1**

| Member ports | 6,2;6,6;8,2;8,6;6,8 |

### DrGroup 1: MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6505 / 6510 / G610</td>
<td>6520</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

**Zone in Fabric_2**

| Member ports | 6,3;6,7;8,3;8,7;6,9 |

---

106 | Fabric-attached MetroCluster Installation and Configuration Guide
### DR Group 1 - Stack 2 at Site_A

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port 6505 / 6510 / G610</th>
<th>6520</th>
<th>G620</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>controller_A_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>controller_A_2 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>bridge_A_2a FC1</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>controller_B_1 port 0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>controller_B_2 port 0a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone in Fabric_1</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1</td>
<td>5,2;5,6;7,2;7,6;5,10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port 6505 / 6510 / G610</th>
<th>6520</th>
<th>G620</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>bridge_A_2b FC1</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>controller_B_2 port 0c</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone in Fabric_2</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1</td>
<td>5,3;5,7;7,3;7,7;5,11</td>
</tr>
</tbody>
</table>
### DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2</td>
<td>6505 / 6510 / G610 controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>G620</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>G620</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>bridge_A_2a FC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>G620</td>
</tr>
</tbody>
</table>

**Zone in Fabric_1**

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOPIC_FC2</td>
</tr>
</tbody>
</table>

### DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>3</td>
<td>6505 / 6510 / G610 controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>G620</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>controller_A_2 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>G620</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>bridge_A_2b FC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>G620</td>
</tr>
</tbody>
</table>

**Zone in Fabric_2**

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOPIC_FC2</td>
</tr>
</tbody>
</table>
### DR Group 1 - Stack 1 at Site_B

**DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1**

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6505 / 6510 / G610</td>
<td>6520</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

**Zone in Fabric_1**

| Member ports **MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1** | 5,2;5,6;7,2;7,6;7,8 |

**DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1**

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6505 / 6510 / G610</td>
<td>6520</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>

**Zone in Fabric_2**

| Member ports **MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1** | 5,3;5,7;7,3;7,7;7,9 |
### DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2 2 2</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 6 6</td>
<td>controller_A_2 port 0b</td>
<td></td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>2 2 2</td>
<td>controller_B_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 6 6</td>
<td>controller_B_2 port 0b</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 8 8</td>
<td>bridge_B_1a FC2</td>
<td></td>
</tr>
</tbody>
</table>

#### Zone in Fabric_1

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2</td>
</tr>
<tr>
<td>6,2;6,6;8,2;8,6;8,8</td>
</tr>
</tbody>
</table>

### DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>3 3 3</td>
<td>controller_A_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 7 7</td>
<td>controller_A_2 port 0b</td>
<td></td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>8</td>
<td>3 3 3</td>
<td>controller_B_1 port 0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 7 7</td>
<td>controller_B_2 port 0b</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 9 9</td>
<td>bridge_A_1b FC2</td>
<td></td>
</tr>
</tbody>
</table>

#### Zone in Fabric_2

<table>
<thead>
<tr>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2</td>
</tr>
<tr>
<td>6,3;6,7;8,3;8,7;8,9</td>
</tr>
</tbody>
</table>
### DR Group 1 - Stack 2 at Site_B

<table>
<thead>
<tr>
<th>DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FC switch</strong></td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>FC_switch_B_1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

#### Zone in Fabric_1

<table>
<thead>
<tr>
<th><strong>Member ports</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1</td>
</tr>
</tbody>
</table>

### DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1

<table>
<thead>
<tr>
<th><strong>FC switch</strong></th>
<th><strong>Site</strong></th>
<th><strong>Switch domain</strong></th>
<th><strong>Switch port</strong></th>
<th><strong>Connects to</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>5</td>
<td>3, 3, 3</td>
<td>controller_A_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7, 7, 7</td>
<td>controller_A_2 port 0c</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td>B</td>
<td>7</td>
<td>3, 3, 3</td>
<td>controller_B_1 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7, 7, 7</td>
<td>controller_B_2 port 0c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11, 11, 11</td>
<td>bridge_B_2b FC1</td>
</tr>
</tbody>
</table>

#### Zone in Fabric_2

<table>
<thead>
<tr>
<th><strong>Member ports</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1</td>
</tr>
</tbody>
</table>
### DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6505 / 6510 / G610</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

### Zone in Fabric_1

<table>
<thead>
<tr>
<th>Member ports</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TO_FC2</td>
<td>6,2;6,6;8,2;8,6;8,10</td>
</tr>
</tbody>
</table>

### DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2

<table>
<thead>
<tr>
<th>FC switch</th>
<th>Site</th>
<th>Switch domain</th>
<th>Switch port</th>
<th>Connects to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>6505 / 6510 / G610</td>
<td>6520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>FC_switch_A_1</td>
<td>A</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>

### Zone in Fabric_2

<table>
<thead>
<tr>
<th>Member ports</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2</td>
<td>6,3;6,7;8,3;8,7;8,11</td>
</tr>
</tbody>
</table>
### Summary of storage zones

<table>
<thead>
<tr>
<th>Fabric</th>
<th>Zone name</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A</td>
<td>MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1</td>
<td>5,2;5,6;7,2;7,6;5,8</td>
</tr>
<tr>
<td>_1 and</td>
<td>FC_switch_B_1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1</td>
<td>5,3;5,7;7,3;7,7;5,9</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1</td>
<td>5,2;5,6;7,2;7,6;5,10</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1</td>
<td>5,3;5,7;7,3;7,7;5,11</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1</td>
<td>5,2;5,6;7,2;7,6;7,8</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1</td>
<td>5,3;5,7;7,3;7,7;7,9</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1</td>
<td>5,2;5,6;7,2;7,6;7,10</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1</td>
<td>5,3;5,7;7,3;7,7;7,11</td>
</tr>
<tr>
<td>FC_switch_A</td>
<td>MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2</td>
<td>6,2;6,6;8,2;8,6;6,8</td>
</tr>
<tr>
<td>_2 and</td>
<td>FC_switch_B_2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC_switch_B_2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC2</td>
<td>6,3;6,7;8,3;8,7;6,9</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC2</td>
<td>6,2;6,6;8,2;8,6;6,10</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC2</td>
<td>6,3;6,7;8,3;8,7;6,11</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2</td>
<td>6,2;6,6;8,2;8,6;8,8</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC2</td>
<td>6,3;6,7;8,3;8,7;8,9</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC2</td>
<td>6,2;6,6;8,2;8,6;8,10</td>
</tr>
<tr>
<td></td>
<td>MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC2</td>
<td>6,3;6,7;8,3;8,7;8,11</td>
</tr>
</tbody>
</table>

### Configuring zoning on Brocade FC switches

You must assign the switch ports to separate zones to separate controller and storage traffic, with zones for the FC-VI ports and zones for the storage ports.

### About this task

The following steps use the standard zoning for the MetroCluster configuration.

Zoning for FC-VI ports on page 95
Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using one FC port on page 98
Zoning for FibreBridge 7500N bridges using both FC ports on page 104

Steps

1. Create the FC-VI zones on each switch:

   
   ```
   zonecreate "QOSH1_FCVI_1", member;member ...
   ```

   
   Example
   
   In this example a QOS FCVI zone is created containing ports 5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5:
   
   ```
   Switch_A_1:admin> zonecreate "QOSH1_FCVI_1", "5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5"
   ```

2. Configure the storage zone s on each switch.

   You can configure zoning for the fabric from one switch in the fabric. In the example that follows, zoning is configured on Switch_A_1.

   a. Create the storage zone for each switch domain in the switch fabric:

   ```
   zonecreate name, member;member ...
   ```

   Example
   
   In this example a storage zone for a FibreBridge 7500N using both FC ports is being created. The zones contains ports 5,2;5,6;7,2;7,6;5,16:
   
   ```
   Switch_A_1:admin> zonecreate "MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
   ```

   b. Create the configuration in the first switch fabric:

   ```
   cfgcreate config_name, zone;zone...
   ```

   Example
   
   In this example a configuration with the name CFG_1 and the two zones QOSH1_MC1_FAB_1_FCVI and MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1 is created
   
   ```
   Switch_A_1:admin> cfgcreate CFG_1, "QOSH1_MC1_FAB_1_FCVI;
   MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
   ```

   c. Add zones to the configuration, if desired:

   ```
   cfgadd config_name zone;zone...
   ```

   d. Enable the configuration:

   ```
   cfgenable config_name
   ```

   Example
   
   ```
   Switch_A_1:admin> cfgenable "CFG_1"
   ```

   e. Save the configuration:

   ```
   cfgsave
   ```
Example

Switch_A_1:admin> cfgsave

f. Validate the zoning configuration:
zone --validate

Example

Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
------------------------
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone

Setting ISL encryption on Brocade 6510 or G620 switches

On Brocade 6510 or G620 switches, you can optionally use the Brocade encryption feature on the ISL connections. If you want to use the encryption feature, you must perform additional configuration steps on each switch in the MetroCluster configuration.

Before you begin

- You must have Brocade 6510 or G620 switches.

  Note: Support for ISL encryption on Brocade G620 switches is only supported on ONTAP 9.4 and later.

- You must have selected two switches from the same fabric.

- You must have reviewed the Brocade documentation for your switch and Fabric Operating System version to confirm the bandwidth and port limits.

About this task

The steps must be performed on both the switches in the same fabric.
Disabling virtual fabric

In order to set the ISL encryption, you must disable the virtual fabric on all the four switches being used in a MetroCluster configuration.

Step

1. Disable the virtual fabric by entering the following command at the switch console:
   
   \texttt{fosconfig --disable vf}

After you finish

Reboot the switch.

Setting the payload

After disabling the virtual fabric, you must set the payload or the data field size on both switches in the fabric.

About this task

The data field size must not exceed 2048.

Steps

1. Disable the switch:
   
   \texttt{switchdisable}

2. Configure and set the payload:
   
   \texttt{configure}

3. Set the following switch parameters:
   
   a. Set the Fabric parameter as follows:
      
      \texttt{y}
   
   b. Set the other parameters, such as Domain, WWN Based persistent PID, and so on.
   
   c. Set the data field size:
      
      \texttt{2048}

Setting the authentication policy

You must set the authentication policy and associated parameters.

About this task

The commands must be executed at the switch console.

Steps

1. Set the authentication secret:
   
   a. Begin the setup process:
      
      \texttt{secAuthSecret --set}
   
      This command initiates a series of prompts that you respond to in the following steps.
   
   b. Provide the worldwide name (WWN) of the other switch in the fabric for the Enter peer WWN, Domain, or switch name parameter.
c. Provide the peer secret for the `Enter peer secret` parameter.
d. Provide the local secret for the `Enter local secret` parameter.
e. Enter `Y` for the `Are you done` parameter.

**Example**

The following is an example of setting the authentication secret:

```
setAuthSecret --set
```

This command is used to set up secret keys for the DH-CHAP authentication.
The minimum length of a secret key is 8 characters and maximum 40 characters. Setting up secret keys does not initiate DH-CHAP authentication. If switch is configured to do DH-CHAP, it is performed whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > <cr>

Enter peer WWN, Domain, or switch name (Leave blank when done):
10:00:00:05:33:76:2e:99
Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter peer WWN, Domain, or switch name (Leave blank when done): 
Are you done? (yes, y, no, n): [no] yes
Saving data to key store... Done.

2. Set the authentication group to 4:
```
authUtil --set -g 4
```

3. Set the authentication type to `dhchap`:
```
authUtil --set -a dhchap
```

The system displays the following output:
```
Authentication is set to dhchap.
```

4. Set the authentication policy on the switch to `on`:
```
authUtil --policy -sw on
```

The system displays the following output:
```
Warning: Activating the authentication policy requires either DH-CHAP secrets or PKI certificates depending on the protocol selected. Otherwise, ISLs will be segmented during next E-port bring-up.
ARE YOU SURE (yes, y, no, n): [no] yes
Auth Policy is set to ON
```
Enabling ISL encryption on Brocade switches

After setting the authentication policy and the authentication secret, you must enable ISL encryption on the ports for it to take effect.

About this task

- These steps should be performed on one switch fabric at a time.
- The commands must be run at the switch console.

Steps

1. Enable encryption on all of the ISL ports:
   
   ```
   portCfgEncrypt --enable port_number
   ```

   Example
   
   In the following example, the encryption is enabled on ports 8 and 12:
   
   ```
   portCfgEncrypt --enable 8
   portCfgEncrypt --enable 12
   ```

2. Enable the switch:
   
   ```
   switchenable
   ```

3. Verify that the ISL is up and working:
   
   ```
   islshow
   ```

4. Verify that encryption is enabled:
   
   ```
   portenccompshow
   ```

   Example
   
   The following example shows that encryption is enabled on ports 8 and 12:
   
<table>
<thead>
<tr>
<th>User Encryption</th>
<th>Port configured</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>8</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>9</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>12</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

After you finish

Perform all of the steps on the switches in the other fabric in a MetroCluster configuration.

Configuring the Cisco FC switches

Each Cisco switch in the MetroCluster configuration must be configured appropriately for the ISL and storage connections.

About this task

The following requirements apply to the Cisco FC switches:
• You must be using four supported Cisco switches of the same model with the same NX-OS version and licensing.

• The MetroCluster configuration requires four switches. The four switches must be connected into two fabrics of two switches each, with each fabric spanning both sites.

• The switch must support connectivity to the ATTO FibreBridge model.

• You cannot be using encryption or compression in the Cisco FC storage fabric. It is not supported in the MetroCluster configuration.

**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.

The following requirement applies to the Inter-Switch Link (ISL) connections:

• All ISLs must have the same length and same speed in one fabric. Different lengths of ISLs can be used in the different fabrics. The same speed must be used in all fabrics.

The following requirement applies to the storage connections:

• Each storage controller must have four initiator ports available to connect to the switch fabrics. Two initiator ports must be connected from each storage controller to each fabric.

  **Note:** You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems with two initiators ports per controller (a single initiator port to each fabric) if all of the following criteria are met:

  ◦ There are fewer than four FC initiator ports available to connect the disk storage and no additional ports can be configured as FC initiators.

  ◦ All slots are in use and no FC initiator card can be added.

**Steps**

1. Cisco switch license requirements on page 120
2. Setting the Cisco FC switch to factory defaults on page 120
3. Configure the Cisco FC switch basic settings and community string on page 121
4. Acquiring licenses for ports on page 122
5. Enabling ports in a Cisco MDS 9148 or 9148S switch on page 123
6. Configuring the F-ports on a Cisco FC switch on page 124
7. Assigning buffer-to-buffer credits to F-Ports in the same port group as the ISL on page 125
8. Creating and configuring VSANs on Cisco FC switches on page 127
9. Configuring E-ports on page 131
10. Configuring zoning on a Cisco FC switch on page 148
11. Ensuring the FC switch configuration is saved on page 150

**Related information**

  *NetApp Interoperability Matrix Tool*
Cisco switch license requirements

Certain feature-based licenses might be required for the Cisco switches in a fabric-attached MetroCluster configuration. These licenses enable you to use features such as QoS or long-distance mode credits on the switches. You must install the required feature-based licenses on all four switches in a MetroCluster configuration.

The following feature-based licenses might be required in a MetroCluster configuration:

- **ENTERPRISE_PKG**
  This license enables you to use the QoS feature on Cisco switches.

- **PORT_ACTIVATION_PKG**
  You can use this license for Cisco 9148 switches. This license enables you to activate or deactivate ports on the switches as long as only 16 ports are active at any given time. By default, 16 ports are enabled in Cisco MDS 9148 switches.

- **FM_SERVER_PKG**
  This license enables you to manage fabrics simultaneously and to manage switches through a web browser.
  The FM_SERVER_PKG license also enables performance management features such as performance thresholds and threshold monitoring. For more information about this license, see the Cisco Fabric Manager Server Package.

You can verify that the licenses are installed by using the `show license usage` command. If you do not have these licenses, contact your sales representative before proceeding with the installation.

**Note:** The Cisco MDS 9250i switches have two fixed 1/10 GbE IP storage services ports. No additional licenses are required for these ports. The Cisco SAN Extension over IP application package is a standard license on these switches that enables features such as FCIP and compression.

Setting the Cisco FC switch to factory defaults

To ensure a successful configuration, you must set the switch to its factory defaults. This ensures that the switch is starting from a clean configuration.

**About this task**

This task must be performed on all switches in the MetroCluster configuration.

**Steps**

1. Make a console connection and log in to both switches in the same fabric.

2. Issue the following command to set the switch back to its default settings:

   ```
   write erase
   ```

   You can respond `y` when prompted to confirm the command. This erases all licenses and configuration information on the switch.

3. Issue the following command to reboot the switch:

   ```
   reload
   ```

   You can respond `y` when prompted to confirm the command.

4. Repeat the `write erase` and `reload` commands on the other switch.

   After issuing the `reload` command, the switch reboots and then prompts with setup questions. At that point, proceed to the next section.
Configure the Cisco FC switch basic settings and community string

You must specify the basic settings with the setup command or after issuing the reload command.

Steps

1. If the switch does not display the setup questions, configure the basic switch settings:

   `setup`

2. Accept the default responses to the setup questions until you are prompted for the SNMP community string.

3. Set the community string to `public` (all lowercase) to allow access from the ONTAP Health Monitors.

   You can set the community string to a value other than `public`, but you must configure the ONTAP Health Monitors using the community string you specify.

Example

The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1# setup
   Configure read-only SNMP community string (yes/no) [n]: y
   SNMP community string : public
   Note: Please set the SNMP community string to "Public" or another value of your choosing.
   Configure default switchport interface state (shut/noshut) [shut]: noshut
   Configure default switchport port mode F (yes/no) [n]: n
   Configure default zone policy (permit/deny) [deny]: deny
   Enable full zoneset distribution? (yes/no) [n]: yes
```

The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1# setup
   Configure read-only SNMP community string (yes/no) [n]: y
   SNMP community string : public
   Note: Please set the SNMP community string to "Public" or another value of your choosing.
   Configure default switchport interface state (shut/noshut) [shut]: noshut
   Configure default switchport port mode F (yes/no) [n]: n
   Configure default zone policy (permit/deny) [deny]: deny
   Enable full zoneset distribution? (yes/no) [n]: yes
```
Acquiring licenses for ports

You do not have to use Cisco switch licenses on a continuous range of ports; instead, you can acquire licenses for specific ports that are used and remove licenses from unused ports. You should verify the number of licensed ports in the switch configuration and, if necessary, move licenses from one port to another as needed.

Steps

1. Issue the following command to show license usage for a switch fabric:
   
   ```
   show port-resources module 1
   ```
   
   Determine which ports require licenses. If some of those ports are unlicensed, determine if you have extra licensed ports and consider removing the licenses from them.

2. Issue the following command to enter configuration mode:

   ```
   config t
   ```

3. Remove the license from the selected port:
   
   a. Issue the following command to select the port to be unlicensed:
      
      ```
      interface interface-name
      ```
   
   b. Remove the license from the port using the following command:
      
      ```
      no port-license acquire
      ```
   
   c. Exit the port configuration interface:
      
      ```
      exit
      ```

4. Acquire the license for the selected port:
   
   a. Issue the following command to select the port to be unlicensed:
      
      ```
      interface interface-name
      ```
   
   b. Make the port eligible to acquire a license using the "port license" command:
      
      ```
      port-license
      ```
   
   c. Acquire the license on the port using the following command:
      
      ```
      port-license acquire
      ```
   
   d. Exit the port configuration interface:
      
      ```
      exit
      ```

5. Repeat for any additional ports.

6. Issue the following command to exit configuration mode:

   ```
   exit
   ```

Removing and acquiring a license on a port

This example shows a license being removed from port fc1/2, port fc1/1 being made eligible to acquire a license, and the license being acquired on port fc1/1:

```
Switch_A_1# conf t
Switch_A_1(config)# interface fc1/2
Switch_A_1(config)# shut
Switch_A_1(config-if)# no port-license acquire
Switch_A_1(config-if)# exit
```
Switch_A_1(config)# interface fc1/1
Switch_A_1(config-if)# port-license
Switch_A_1(config-if)# port-license acquire
Switch_A_1(config-if)# no shut
Switch_A_1(config-if)# end
Switch_A_1# copy running-config startup-config

Switch_B_1# conf t
Switch_B_1(config)# interface fc1/2
Switch_B_1(config)# shut
Switch_B_1(config-if)# no port-license acquire
Switch_B_1(config-if)# exit
Switch_B_1(config)# interface fc1/1
Switch_B_1(config-if)# port-license
Switch_B_1(config-if)# port-license acquire
Switch_B_1(config-if)# no shut
Switch_B_1(config-if)# end
Switch_B_1# copy running-config startup-config

The following example shows port license usage being verified:

Switch_A_1# show port-resources module 1
Switch_B_1# show port-resources module 1

Enabling ports in a Cisco MDS 9148 or 9148S switch

In Cisco MDS 9148 or 9148S switches, you must manually enable the ports required in a MetroCluster configuration.

About this task

- You can manually enable 16 ports in a Cisco MDS 9148 or 9148S switch.
- The Cisco switches enable you to apply the POD license on random ports, as opposed to applying them in sequence.
- Cisco switches require that you use one port from each port group, unless you need more than 12 ports.

Steps

1. View the port groups available in a Cisco switch:
   
   `show port-resources module blade_number`

2. License and acquire the required port in a port group by entering the following commands in sequence:
   
   `config t`
   `interface port_number`
   `shut`
   `port-license acquire`
   `no shut`

Example

For example, the following command licenses and acquires Port fc 1/45:
Switch# config t
switch(config)#
switch(config)# interface fc 1/45
switch(config-if)#
switch(config-if)# shut
switch(config-if)# port-license acquire
switch(config-if)# no shut
switch(config-if)# end

3. Save the configuration:
   copy running-config startup-config

Configuring the F-ports on a Cisco FC switch

You must configure the F-ports on the FC switch. In a MetroCluster configuration, the F-ports are the ports that connect the switch to the HBA initiators, FC-VI interconnects and FC-to-SAS bridges. Each port must be configured individually.

About this task

Refer to the following sections to identify the F-ports (switch-to-node) for your configuration:

- Port assignments for FC switches when using ONTAP 9.1 and later on page 52
- Port assignments for FC switches when using ONTAP 9.0 on page 37

This task must be performed on each switch in the MetroCluster configuration.

Steps

1. Issue the following command to enter configuration mode:
   config t

2. Enter interface configuration mode for the port:
   interface port-ID

3. Shut down the port:
   shutdown

4. Set the ports to F mode by issuing the following command:
   switchport mode F

5. Set the ports to fixed speed by issuing the following command:
   switchport speed speed
   speed is either 8000 or 16000

6. Set the rate mode of the switch port to dedicated by issuing the following command:
   switchport rate-mode dedicated

7. Restart the port:
   no shutdown

8. Issue the following command to exit configuration mode:
   end

The following example shows the commands on the two switches:
Assigning buffer-to-buffer credits to F-Ports in the same port group as the ISL

You must assign the buffer-to-buffer credits to the F-ports if they are in the same port group as the ISL. If the ports do not have the required buffer-to-buffer credits, the ISL could be inoperative. This task is not required if the F-ports are not in the same port group as the ISL port.

About this task

If the F-Ports are in a port group that contains the ISL, this task must be performed on each FC switch in the MetroCluster configuration.

Steps

1. Issue the following command to enter configuration mode:
   ```
   config t
   ```

2. Enter the following command to set the interface configuration mode for the port:
   ```
   interface port-ID
   ```

3. Disable the port:
   ```
   shut
   ```

4. If the port is not already in F mode, set the port to F mode by entering the following command:
   ```
   switchport mode F
   ```

5. Set the buffer-to-buffer credit of the non-E ports to 1 by using the following command:
   ```
   switchport fcrxbbcredit 1
   ```

6. Re-enable the port:
   ```
   no shut
   ```

7. Exit configuration mode:
   ```
   exit
   ```

8. Copy the updated configuration to the startup configuration:
   ```
   copy running-config startup-config
   ```

9. Verify the buffer-to-buffer credit assigned to a port by entering the following commands:
   ```
   show port-resources module 1
   ```
10. Issue the following command to exit configuration mode:
   ```
   exit
   ```

11. Repeat these steps on the other switch in the fabric.

12. Verify the settings:
   ```
   show port-resource module 1
   ```

In this example, port fc1/40 is the ISL. Ports fc1/37, fc1/38 and fc1/39 are in the same port group and must be configured.

The following commands show the port range being configured for fc1/37 through fc1/39:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrrxb credit 1
FC_switch_B_1(config-if)# no shut
FC_switch_B_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

The following commands and system output show that the settings are properly applied:

```
FC_switch_A_1# show port-resource module 1
...  
Port-Group 11
    Available dedicated buffers are 93

       Interfaces in the Port-Group          B2B Credit  Bandwidth  Rate Mode
                      Buffers     (Gbps)          
-----------------------------  -----------------  -------------------  
fc1/37                        32             8.0        dedicated
fc1/38                        1              8.0        dedicated
fc1/39                        1              8.0        dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
    Available dedicated buffers are 93

       Interfaces in the Port-Group          B2B Credit  Bandwidth  Rate Mode
                      Buffers     (Gbps)          
-----------------------------  -----------------  -------------------  
fc1/37                        32             8.0        dedicated
fc1/38                        1              8.0        dedicated
fc1/39                        1              8.0        dedicated
...
Creating and configuring VSANs on Cisco FC switches

You must create a VSAN for the FC-VI ports and a VSAN for the storage ports on each FC switch in the MetroCluster configuration. The VSANs should have a unique number and name. You must do additional configuration if you are using two ISLs with in-order delivery of frames.

About this task

The examples here use the following naming conventions:

<table>
<thead>
<tr>
<th>Switch fabric</th>
<th>VSAN name</th>
<th>ID number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FCVI_1_10</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>STOR_1_20</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>FCVI_2_30</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>STOR_2_20</td>
<td>40</td>
</tr>
</tbody>
</table>

This task must be performed on each FC switch fabric.

Steps

1. Configure the FC-VI VSAN:
   a. Enter configuration mode if you have not done so already:
      ```
cfg t
```
   b. Edit the VSAN database:
      ```
vSAN database
```
   c. Set the VSAN ID:
      ```
vSAN vsan-ID
```
   d. Set the VSAN name:
      ```
vSAN vsan-ID name vsan_name
```

2. Add ports to the FC-VI VSAN:
   a. Add the interfaces for each port in the VSAN:
      ```
vSAN vsan-ID interface interface_name
```
      For the FC-VI VSAN, the ports connecting the local FC-VI ports will be added.
   b. Exit configuration mode:
      ```
end
```
   c. Copy the running-config to the startup-config:
      ```
copy running-config startup-config
```

Example

In the following example, the ports are fc1/1 and fc1/13:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
```
3. Verify port membership of the VSAN:

   show vsan member

**Example**

```
FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member
```

4. Configure the VSAN to guarantee in-order delivery of frames or out-of-order delivery of frames:

   **Note:** The standard IOD settings are recommended. You should configure OOD only if necessary.

   Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations on page 14

   - The following steps must be performed to configure in-order delivery of frames:
     a. Enter configuration mode:
        ```
        conf t
        ```
     b. Enable the in-order guarantee of exchanges for the VSAN:
        ```
        in-order-guarantee vsan vsan-ID
        ```
        **Attention:** For FC-VI VSANs (FCVI_1_10 and FCVI_2_30), you must enable in-order guarantee of frames and exchanges only on VSAN 10.
     c. Enable load balancing for the VSAN:
        ```
        vsan vsan-ID loadbalancing src-dst-id
        ```
     d. Exit configuration mode:
        ```
        end
        ```
     e. Copy the running-config to the startup-config:
        ```
        copy running-config startup-config
        ```

The commands to configure in-order delivery of frames on FCSwitch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to configure in-order delivery of frames on FCSwitch_B_1:

```
The following steps must be performed to configure out-of-order delivery of frames:

a. Enter configuration mode:

   ```
   conf t
   ```

b. Disable the in-order guarantee of exchanges for the VSAN:

   ```
   no in-order-guarantee vsan vsan-ID
   ```

c. Enable load balancing for the VSAN:

   ```
   vsan vsan-ID loadbalancing src-dst-id
   ```

d. Exit configuration mode:

   ```
   end
   ```

e. Copy the running-config to the startup-config:

   ```
   copy running-config startup-config
   ```

The commands to configure out-of-order delivery of frames on FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to configure out-of-order delivery of frames on FC_switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

**Note:** When configuring ONTAP on the controller modules, OOD must be explicitly configured on each controller module in the MetroCluster configuration.

*Configuring in-order delivery or out-of-order delivery of frames on ONTAP software* on page 208

5. Set QoS policies for the FC-VI VSAN:

a. Enter configuration mode:

   ```
   conf t
   ```

b. Enable the QoS and create a class map by entering the following commands in sequence:

   ```
   qos enable
   qos class-map class_name match-any
   ```

c. Add the class map created in a previous step to the policy map:

   ```
   class class_name
   ```
d. Set the priority:
   \texttt{priority high}

e. Add the VSAN to the policy map created previously in this procedure:
   \texttt{qos service policy policy\_name vsan vsanid}

f. Copy the updated configuration to the startup configuration:
   \texttt{copy running-config startup-config}

\textbf{Example}

The commands to set the QoS policies on FC\_switch\_A\_1:

```bash
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI\_1\_10\_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI\_1\_10\_Policy
FC_switch_A_1(config-pmap)# class FCVI\_1\_10\_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# qos service policy FCVI\_1\_10\_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to set the QoS policies on FC\_switch\_B\_1:

```bash
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI\_1\_10\_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI\_1\_10\_Policy
FC_switch_B_1(config-pmap)# class FCVI\_1\_10\_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# qos service policy FCVI\_1\_10\_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

6. Configure the storage VSAN:

a. Set the VSAN ID:
   \texttt{vsan vsan\_ID}

b. Set the VSAN name:
   \texttt{vsan vsan\_ID name vsan\_name}

\textbf{Example}

The commands to configure the storage VSAN on FC\_switch\_A\_1:

```bash
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR\_1\_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to configure the storage VSAN on FC\_switch\_B\_1:

```bash
```
7. Add ports to the storage VSAN.

For the storage VSAN, all ports connecting HBA or FC-to-SAS bridges must be added. In this example fc1/5, fc1/9, fc1/17, fc1/21, fc1/25, fc1/29, fc1/33, and fc1/37 are being added.

Example

The commands to add ports to the storage VSAN on FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to add ports to the storage VSAN on FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

**Configuring E-ports**

You must configure the switch ports that connect the ISL (these are the E-Ports). The procedure you use depends on which switch you are using.

**Configuring the E-ports on the Cisco FC switch**

You must configure the FC switch ports that connect the inter-switch link (ISL). These are the E-ports, and configuration must be done for each port. To do so, you must calculate the correct number of buffer-to-buffer credits (BBCs).

**About this task**

All ISLs in the fabric must be configured with the same speed and distance settings.

This task must be performed on each ISL port.
Steps

1. Use the following table to determine the adjusted required BBCs per kilometer for possible port speeds.

To determine the correct number of BBCs, you multiply the Adjusted BBCs required (determined from the following table) by the distance in kilometers between the switches. An adjustment factor of 1.5 is required to account for FC-VI framing behavior.

<table>
<thead>
<tr>
<th>Speed in Gbps</th>
<th>BBCs required per kilometer</th>
<th>Adjusted BBCs required (BBCs per km x 1.5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.5</td>
<td>0.75</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1.5</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
<td>12</td>
</tr>
</tbody>
</table>

Example

For example, to compute the required number of credits for a distance of 30 km on a 4-Gbps link, make the following calculation:

- Speed in Gbps is 4
- Adjusted BBCs required is 3
- Distance in kilometers between switches is 30 km
- 3 x 30 = 90

2. Issue the following command to enter configuration mode:

   config t

3. Specify the port you are configuring:

   interface port-name

4. Shut down the port:

   shutdown

5. Set the rate mode of the port to dedicated:

   switchport rate-mode dedicated

6. Set the speed for the port:

   switchport speed speed

7. Set the buffer-to-buffer credits for the port:

   switchport fcxbbbccredit number of buffers

8. Set the port to E mode:

   switchport mode E

9. Enable the trunk mode for the port:

   switchport trunk mode on

10. Add the ISL virtual storage area networks (VSANs) to the trunk:

    switchport trunk allowed vsan 10
switchport trunk allowed vsan add 20

11. Add the port to port channel 1:

channel-group 1

12. Repeat the previous steps for the matching ISL port on the partner switch in the fabric.

Example

The following example shows port fc1/41 configured for a distance of 30 km and 8 Gbps:

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

13. Issue the following command on both switches to restart the ports:

```
no shutdown
```

14. Repeat the previous steps for the other ISL ports in the fabric.

15. Add the native VSAN to the port-channel interface on both switches in the same fabric:

```
interface port-channel number

switchport trunk allowed vsan add native_san_id
```

16. Verify configuration of the port-channel:

```
show interface port-channel number
```

The port channel should have the following attributes:

- The port-channel is trunking.
- Admin port mode is E, trunk mode is on.
- Speed shows the cumulative value of all the ISL link speeds.
  For example, two ISL ports operating at 4 Gbps should show a speed of 8 Gbps.
- Trunk vsans (admin allowed and active) shows all the allowed VSANs.
- Trunk vsans (up) shows all the allowed VSANs.
- The member list shows all the ISL ports that were added to the port-channel.
- The port VSAN number should be the same as the VSAN that contains the ISLs (usually native vsan 1).
17. Exit interface configuration on both switches:

    end

18. Copy the updated configuration to the startup configuration on both fabrics:

    copy running-config startup-config

Example

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config
```

19. Repeat the previous steps on the second switch fabric.

Related concepts

- Port assignments for FC switches when using ONTAP 9.1 and later on page 52

**Configuring FCIP ports for a single ISL on Cisco 9250i FC switches**

You must configure the FCIP switch ports that connect the ISL (E-ports) by creating FCIP profiles and interfaces, and then assigning them to the IPStorage1/1 GbE interface.

About this task

This task is only for configurations using a single ISL per switch fabric, using the IPStorage1/1 interface on each switch.

This task must be performed on each FC switch.

Two FCIP profiles are created on each switch:
• Fabric 1
  ◦ FC_switch_A_1 is configured with FCIP profiles 11 and 111.
  ◦ FC_switch_B_1 is configured with FCIP profiles 12 and 121.
• Fabric 2
  ◦ FC_switch_A_2 is configured with FCIP profiles 13 and 131.
  ◦ FC_switch_B_2 is configured with FCIP profiles 14 and 141.

Steps
1. Enter configuration mode:
config t
2. Enable FCIP:
feature fcip
3. Configure the IPStorage1/1 GbE interface:
   a. Enter configuration mode:
      config t
   b. Specify the IPStorage1/1 interface:
      interface IPStorage1/1
   c. Specify the IP address and subnet mask:
      interface ip-address subnet-mask
   d. Specify the MTU size of 2500:
      switchport mtu 2500
   e. Enable the port:
      no shutdown
   f. Exit configuration mode:
      exit

Example
The following example shows the configuration of an IPStorage1/1 port:

```bash
conf t
interface IPStorage1/1
  ip address 192.168.1.201 255.255.255.0
  switchport mtu 2500
  no shutdown
exit
```
4. Configure the FCIP profile for FC-VI traffic:
   a. Configure an FCIP profile and enter FCIP profile configuration mode:
      fcip profile FCIP-profile-name
      The profile name depends on which switch is being configured.
   b. Assign the IP address of the IPStorage1/1 interface to the FCIP profile:
      ip address ip-address
c. Assign the FCIP profile to TCP port 3227:
   
   ```
   port 3227
   ```

d. Set the TCP settings:
   
   ```
   tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm
   ```

**Example**

The following example shows the configuration of the FCIP profile:

```bash
conf t
fcip profile 11
   ip address 192.168.1.333
   port 3227
   tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm
```

5. Configure the FCIP profile for storage traffic:

a. Configure an FCIP profile with the name 111 and enter FCIP profile configuration mode:
   
   ```
   fcip profile 111
   ```

b. Assign the IP address of the IPStorage1/1 interface to the FCIP profile:
   
   ```
   ip address ip-address
   ```

c. Assign the FCIP profile to TCP port 3229:
   
   ```
   port 3229
   ```

d. Set the TCP settings:
   
   ```
   tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm
   ```
Example

The following example shows the configuration of the FCIP profile:

```bash
conf t
fcip profile 111
   ip address 192.168.1.334
   port 3229
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm
```

6. Create the first of two FCIP interfaces:

```bash
interface fcip 1
This interface is used for FC-IV traffic.
a. Select the profile 11 created previously:
   use-profile 11
b. Set the IP address and port of the IPStorage1/1 port on the partner switch:
   peer-info ipaddr partner-switch-port-ip port 3227
c. Select TCP connection 2:
   tcp-connection 2
d. Disable compression:
   no ip-compression
e. Enable the interface:
   no shutdown
f. Configure the control TCP connection to 48 and the data connection to 26 to mark all packets on that differentiated services code point (DSCP) value:
   qos control 48 data 26
g. Exit the interface configuration mode:
   exit
```

Example

The following example shows the configuration of the FCIP interface:

```bash
interface fcip 1
use-profile 11
# the port # listed in this command is the port that the remote switch is listening on
peer-info ipaddr 192.168.32.334 port 3227
tcp-connection 2
no ip-compression
no shutdown
qos control 48 data 26
exit
```

7. Create the second of two FCIP interfaces:
interface fcip 2

This interface is used for storage traffic.

a. Select the profile 111 created previously:
   use-profile 111

b. Set the IP address and port of the IPStorage1/1 port on the partner switch:
   peer-info ipaddr partner-switch-port-ip port 3229

c. Select TCP connection 2:
   tcp-connection 5

d. Disable compression:
   no ip-compression

e. Enable the interface:
   no shutdown

f. Configure the control TCP connection to 48 and data connection to 26 to mark all packets on
   that differentiated services code point (DSCP) value:
   qos control 48 data 26

g. Exit the interface configuration mode:
   exit

Example

The following example shows the configuration of the FCIP interface:

```
interface fcip 2
use-profile 11
# the port # listed in this command is the port that the remote switch is listening on
peer-info ipaddr 192.168.32.33e port 3229
tcp-connection 5
no ip-compression
no shutdown
qos control 48 data 26
exit
```

8. Configure the switchport settings on the fcip 1 interface:

a. Enter configuration mode:
   config t

b. Specify the port you are configuring:
   interface fcip 1

c. Shut down the port:
   shutdown

d. Set the port to E mode:
   switchport mode E

e. Enable the trunk mode for the port:
   switchport trunk mode on

f. Set the trunk allowed vsan to 10:
switchport trunk allowed vsan 10

g. Set the speed for the port:
switchport speed speed

9. Configure the switchport settings on the fcip 2 interface:
a. Enter configuration mode:
   config t
b. Specify the port you are configuring:
   interface fcip 2
c. Shut down the port:
   shutdown
d. Set the port to E mode:
   switchport mode E
e. Enable the trunk mode for the port:
   switchport trunk mode on
f. Set the trunk allowed vsan to 20:
   switchport trunk allowed vsan 20
g. Set the speed for the port:
   switchport speed speed

10. Repeat the previous steps on the second switch.

   The only differences are the appropriate IP addresses and unique FCIP profile names.
   • When configuring the first switch fabric, FC_switch_B_1 is configured with FCIP profiles 12 and 121.
   • When configuring the first switch fabric, FC_switch_A_2 is configured with FCIP profiles 13 and 131 and FC_switch_B_2 is configured with FCIP profiles 14 and 141.

11. Restart the ports on both switches:
    no shutdown

12. Exit the interface configuration on both switches:
    end

13. Copy the updated configuration to the startup configuration on both switches:
    copy running-config startup-config

Example

    FC_switch_A_1(config-if)# end
    FC_switch_A_1# copy running-config startup-config

    FC_switch_B_1(config-if)# end
    FC_switch_B_1# copy running-config startup-config

14. Repeat the previous steps on the second switch fabric.
Configuring FCIP ports for a dual ISL on Cisco 9250i FC switches

You must configure the FCIP switch ports that connect the ISL (E-ports) by creating FCIP profiles and interfaces, and then assigning them to the IPStorage1/1 and IPStorage1/2 GbE interfaces.

About this task

This task is only for configurations that use a dual ISL per switch fabric, using the IPStorage1/1 and IPStorage1/2 GbE interfaces on each switch.

This task must be performed on each FC switch.

The task and examples use the following profile configuration table:

<table>
<thead>
<tr>
<th>Switch fabric</th>
<th>IPStor age interface</th>
<th>IP Address</th>
<th>Port type</th>
<th>FCIP interface</th>
<th>FCIP profile</th>
<th>Port</th>
<th>Peer IP/ port</th>
<th>VSAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC_switch_A _1</td>
<td>IPStor age1/1</td>
<td>a.a.a.a</td>
<td>FC-VI</td>
<td>fcip 1</td>
<td>15</td>
<td>3220</td>
<td>c.c.c.c /3230</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 2</td>
<td>20</td>
<td>3221</td>
<td>c.c.c.c /3231</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>IPStor age1/2</td>
<td>b.b.b.b</td>
<td>FC-VI</td>
<td>fcip 3</td>
<td>25</td>
<td>3222</td>
<td>d.d.d.d /3232</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 4</td>
<td>30</td>
<td>3223</td>
<td>d.d.d.d /3233</td>
<td>20</td>
</tr>
<tr>
<td>FC_switch_B _1</td>
<td>IPStor age1/1</td>
<td>c.c.c.c</td>
<td>FC-VI</td>
<td>fcip 1</td>
<td>15</td>
<td>3230</td>
<td>a.a.a.a /3220</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 2</td>
<td>20</td>
<td>3231</td>
<td>a.a.a.a /3221</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>IPStor age1/2</td>
<td>d.d.d.d</td>
<td>FC-VI</td>
<td>fcip 3</td>
<td>25</td>
<td>3232</td>
<td>b.b.b.b /3222</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 4</td>
<td>30</td>
<td>3233</td>
<td>b.b.b.b /3223</td>
<td>20</td>
</tr>
<tr>
<td>Fabric 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Switch Configurations

<table>
<thead>
<tr>
<th>Switch fabric</th>
<th>IPStorage interface</th>
<th>IP Address</th>
<th>Port type</th>
<th>FCIP interface</th>
<th>FCIP profile</th>
<th>Port</th>
<th>Peer IP/port</th>
<th>VSAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A</td>
<td>IPStorage1/1</td>
<td>e.e.e.e.e</td>
<td>FC-VI</td>
<td>fcip 1</td>
<td>15</td>
<td>3220</td>
<td>g.g.g.g</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 2</td>
<td>20</td>
<td>3221</td>
<td>g.g.g.g</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>IPStorage1/2</td>
<td>f.f.f.f.f</td>
<td>FC-VI</td>
<td>fcip 3</td>
<td>25</td>
<td>3222</td>
<td>h.h.h.h</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 4</td>
<td>30</td>
<td>3223</td>
<td>h.h.h.h</td>
<td>20</td>
</tr>
<tr>
<td>FC_switch_B</td>
<td>IPStorage1/1</td>
<td>g.g.g.g.g</td>
<td>FC-VI</td>
<td>fcip 1</td>
<td>15</td>
<td>3230</td>
<td>e.e.e.e</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 2</td>
<td>20</td>
<td>3231</td>
<td>e.e.e.e</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>IPStorage1/2</td>
<td>h.h.h.h.h</td>
<td>FC-VI</td>
<td>fcip 3</td>
<td>25</td>
<td>3232</td>
<td>f.f.f.f</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td>fcip 4</td>
<td>30</td>
<td>3233</td>
<td>f.f.f.f</td>
<td>20</td>
</tr>
</tbody>
</table>

### Steps

1. Enter configuration mode:
   ```
   config t
   ```
2. Enable FCIP:
   ```
   feature fcip
   ```
3. On each switch, configure the two IPStorage interfaces (IPStorage1/1 and IPStorage1/2):
   a. Enter configuration mode:
   ```
   conf t
   ```
   b. Specify the IPStorage interface to create:
   ```
   interface ipstorage
   ```
   The `ipstorage` parameter value is `IPStorage1/1` or `IPStorage1/2`.
   c. Specify the IP address and subnet mask of the IPStorage interface previously specified:
   ```
   interface ip-address subnet-mask
   ```
   **Note:** On each switch, the IPStorage interfaces IPStorage1/1 and IPStorage1/2 must have different IP addresses.
   d. Specify the MTU size as `2500`:
   ```
   switchport mtu 2500
   ```
   e. Enable the port:
   ```
   no shutdown
   ```
   f. Exit configuration mode:
Repeat steps a on page 141 through f on page 141 to configure the IPStorage1/2 GbE interface with a different IP address.

4. Configure the FCIP profiles for FC-VI and storage traffic with the profile names given in the profile configuration table:
   a. Enter configuration mode:
      ```
      conf t
      ```
   b. Configure the FCIP profiles with the following profile names:
      ```
      fcip profile FCIP-profile-name
      ```
      The following list provides the values for the FCIP-profile-name parameter:
      - 15 for FC-VI on IPStorage1/1
      - 20 for storage on IPStorage1/1
      - 25 for FC-VI on IPStorage1/2
      - 30 for storage on IPStorage1/2
   c. Assign the FCIP profile ports according to the profile configuration table:
      ```
      port port number
      ```
   d. Set the TCP settings:
      ```
      tcp keepalive-timeout 1
      tcp max-retransmissions 3
      max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
      tcp min-retransmit-time 200
      tcp keepalive-timeout 1
      tcp pmtu-enable reset-timeout 3600
      tcp sack-enable
      no tcp cwm
      ```

5. Create FCIP interfaces:
   ```
   interface fcip FCIP interface
   ```
   The FCIP interface parameter value is 1, 2, 3, or 4 as given in the profile configuration table.
   a. Map interfaces to the previously created profiles:
      ```
      use-profile profile
      ```
   b. Set the peer IP address and peer profile port number:
      ```
      peer-info peer IPstorage ipaddr peer profile port number
      ```
   c. Select the TCP connections:
      ```
      tcp-connection connection #
      ```
      The connection # parameter value is 2 for FC-VI profiles and 5 for storage profiles.
   d. Disable compression:
      ```
      no ip-compression
      ```
e. Enable the interface:
   
   no shutdown

f. Configure the control TCP connection to 48 and the data connection to 26 to mark all packets that have differentiated services code point (DSCP) value:
   
   qos control 48 data 26

g. Exit configuration mode:
   
   exit

6. Configure the switchport settings on each FCIP interface:
   
   a. Enter configuration mode:
      
      config t

   b. Specify the port that you are configuring:
      
      interface fcip 1

   c. Shut down the port:
      
      shutdown

   d. Set the port to E mode:
      
      switchport mode E

   e. Enable the trunk mode for the port:
      
      switchport trunk mode on

   f. Specify the trunk that is allowed on a specific VSAN:
      
      switchport trunk allowed vsan vsan

      The vsan parameter value is VSAN 10 for FC-VI profiles and VSAN 20 for storage profiles.

   g. Set the speed for the port:
      
      switchport speed speed

   h. Exit configuration mode:
      
      exit

7. Copy the updated configuration to the startup configuration on both switches:
   
   copy running-config startup-config

---

The following examples show the configuration of FCIP ports for a dual ISL in fabric 1 switches FC_switch_A_1 and FC_switch_B_1.

For FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings
feature fcip
conf t
interface IPStorage1/1
# IP address: a.a.a.a
# Mask: y.y.y.y
  ip address <a.a.a.a y.y.y.y>
```
switchport mtu 2500
no shutdown
exit
cconf t
fcip profile 15
   ip address <a.a.a.a>
   port 3220
   tcp keepalive-timeout 1
   tcp max-retransmissions 3
   max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
   tcp min-retransmit-time 200
   tcp keepalive-timeout 1
   tcp pmtu-enable reset-timeout 3600
   tcp sack-enable
   no tcp cwm

ccconf t
fcip profile 20
   ip address <a.a.a.a>
   port 3221
   tcp keepalive-timeout 1
   tcp max-retransmissions 3
   max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
   tcp min-retransmit-time 200
   tcp keepalive-timeout 1
   tcp pmtu-enable reset-timeout 3600
   tcp sack-enable
   no tcp cwm

conf t
interface IPStorage1/2
   # IP address:  b.b.b.b
   # Mask:  y.y.y.y
   ip address <b.b.b.b   y.y.y.y>
   switchport mtu 2500
   no shutdown
   exit

conf t
fcip profile 25
   ip address <b.b.b.b>
   port 3222
   tcp keepalive-timeout 1
   tcp max-retransmissions 3
   max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
   tcp min-retransmit-time 200
   tcp keepalive-timeout 1
   tcp pmtu-enable reset-timeout 3600
   tcp sack-enable
   no tcp cwm

conf t
fcip profile 30
   ip address <b.b.b.b>
   port 3223
   tcp keepalive-timeout 1
   tcp max-retransmissions 3
   max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
   tcp min-retransmit-time 200
   tcp keepalive-timeout 1
   tcp pmtu-enable reset-timeout 3600
   tcp sack-enable
   no tcp cwm

interface fcip 1
   use-profile 15
   # the port # listed in this command is the port that the remote switch is
   # listening on
   peer-info ipaddr <c.c.c.c>  port 3230
   tcp-connection 2
   no ip-compression
   no shutdown
   qos control 48 data 26
   exit

interface fcip 2
   use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
peer-info ipaddr <c.c.c.c>  port 3231
tcp-connection 5
no ip-compression
no shutdown
qos control 48 data 26
exit

interface fcip 3
use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
peer-info ipaddr <d.d.d.d>  port 3232
tcp-connection 2
no ip-compression
no shutdown
qos control 48 data 26
exit

interface fcip 4
use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
peer-info ipaddr <d.d.d.d>  port 3233
tcp-connection 5
no ip-compression
no shutdown
qos control 48 data 26
exit

conf t
interface fcip 1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip 2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip 3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip 4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

For FC_switch_B_1:

FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings
feature fcip
conf t
interface IPStorage1/1
  # IP address:  c.c.c.c
  # Mask:  y.y.y.y
  ip address <c.c.c.c  y.y.y.y>
  switchport mtu 2500
  no shutdown
  exit

conf t
fcip profile 15
  ip address <c.c.c.c>
  port 3230
  tcp keepalive-timeout 1
  tcp max-retransmissions 3
  max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <c.c.c.c>
  port 3231
  tcp keepalive-timeout 1
  tcp max-retransmissions 3
  max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
  # IP address:  d.d.d.d
  # Mask:  y.y.y.y
  ip address <b.b.b.b  y.y.y.y>
  switchport mtu 2500
  no shutdown
  exit

conf t
fcip profile 25
  ip address <d.d.d.d>
  port 3232
  tcp keepalive-timeout 1
  tcp max-retransmissions 3
  max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <d.d.d.d>
  port 3233
  tcp keepalive-timeout 1
  tcp max-retransmissions 3
  max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

interface fcip 1
  use-profile 15
  # the port # listed in this command is the port that the remote switch is listening on
  peer-info ipaddr <a.a.a.a> port 3220
interface fcip 2
  use-profile 20
  # the port # listed in this command is the port that the remote switch is
  listening on
  peer-info ipaddr <a.a.a.a> port 3221
tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
  exit

interface fcip 3
  use-profile 25
  # the port # listed in this command is the port that the remote switch is
  listening on
  peer-info ipaddr <b.b.b.b> port 3222
tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
  exit

interface fcip 4
  use-profile 30
  # the port # listed in this command is the port that the remote switch is
  listening on
  peer-info ipaddr <b.b.b.b> port 3223
tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
  exit

conf t
interface fcip 1
  shutdown
  switchport mode E
  switchport trunk mode on
  switchport trunk allowed vsan 10
  no shutdown
  exit

conf t
interface fcip 2
  shutdown
  switchport mode E
  switchport trunk mode on
  switchport trunk allowed vsan 20
  no shutdown
  exit

conf t
interface fcip 3
  shutdown
  switchport mode E
  switchport trunk mode on
  switchport trunk allowed vsan 10
  no shutdown
  exit

conf t
interface fcip 4
  shutdown
  switchport mode E
  switchport trunk mode on
  switchport trunk allowed vsan 20
  no shutdown
  exit
Configuring zoning on a Cisco FC switch

You must assign the switch ports to separate zones to isolate storage (HBA) and controller (FC-VI) traffic.

About this task

These steps must be performed on both FC switch fabrics.

The following steps use the zoning described in the section Zoning for a FibreBridge 7500N in a four-node MetroCluster configuration.

Zoning for FC-VI ports on page 95

Steps

1. Clear the existing zones and zone set, if present.
   a. Determine which zones and zone sets are active:
      
      \[
      \text{show zoneset active}
      \]

      \[
      \begin{array}{l}
      \text{FC_switch_A_1# show zoneset active} \\
      \text{FC_switch_B_1# show zoneset active}
      \end{array}
      \]

   b. Disable the active zone sets identified in the previous step:
      
      \[
      \text{no zoneset activate name zoneset_name vsan vsan_id}
      \]

      \[
      \begin{array}{l}
      \text{Example} \\
      \text{The following example shows two zone sets being disabled:} \\
      \text{• ZoneSet_A on FC_switch_A_1 in VSAN 10} \\
      \text{• ZoneSet_B on FC_switch_B_1 in VSAN 20}
      \end{array}
      \]

      \[
      \begin{array}{l}
      \text{FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10} \\
      \text{FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20}
      \end{array}
      \]

   c. After all zone sets are deactivated, clear the zone database:
      
      \[
      \text{clear zone database zone-name}
      \]

      \[
      \begin{array}{l}
      \text{Example} \\
      \text{The following example clears the zone database and copies the configuration:} \\
      \text{FC_switch_A_1# clear zone database 10} \\
      \text{FC_switch_A_1# copy running-config startup-config} \\
      \text{FC_switch_B_1# clear zone database 20} \\
      \text{FC_switch_B_1# copy running-config startup-config}
      \end{array}
      \]

2. Obtain the switch worldwide name (WWN):
   
   \[
   \text{show wwn switch}
   \]

3. Configure the basic zone settings:
   a. Set the default zoning policy to \textbf{permit}:
no system default zone default-zone permit

b. Enable the full zone distribution:

    system default zone distribute full

c. Set the default zoning policy for each VSAN:

    no zone default-zone permit vsanid

d. Set the default full zone distribution for each VSAN:

    zoneset distribute full vsanid

Example

<table>
<thead>
<tr>
<th>FC_switch_A_1# conf t</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1(config)# no system default zone default-zone permit</td>
</tr>
<tr>
<td>FC_switch_A_1(config)# system default zone distribute full</td>
</tr>
<tr>
<td>FC_switch_A_1(config)# no zone default-zone permit 10</td>
</tr>
<tr>
<td>FC_switch_A_1(config)# zoneset distribute full vsan 10</td>
</tr>
<tr>
<td>FC_switch_A_1(config)# zoneset distribute full vsan 20</td>
</tr>
<tr>
<td>FC_switch_A_1(config)# end</td>
</tr>
<tr>
<td>FC_switch_A_1# copy running-config startup-config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FC_switch_B_1# conf t</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_B_1(config)# no system default zone default-zone permit</td>
</tr>
<tr>
<td>FC_switch_B_1(config)# system default zone distribute full</td>
</tr>
<tr>
<td>FC_switch_B_1(config)# no zone default-zone permit 10</td>
</tr>
<tr>
<td>FC_switch_B_1(config)# zoneset distribute full vsan 10</td>
</tr>
<tr>
<td>FC_switch_B_1(config)# zoneset distribute full vsan 20</td>
</tr>
<tr>
<td>FC_switch_B_1(config)# end</td>
</tr>
<tr>
<td>FC_switch_B_1# copy running-config startup-config</td>
</tr>
</tbody>
</table>

4. Create storage zones and add the storage ports to them.

These steps only need to be performed on one switch in each fabric.

The zoning depends on the model FC-to-SAS bridge you are using. For details, see the section for your model bridge. The examples show Brocade switch ports, so adjust your ports accordingly.

- **Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using one FC port** on page 98
- **Zoning for FibreBridge 7500N bridges using both FC ports** on page 104

Each storage zone contains the HBA initiator ports from all controllers and one single port connecting an FC-to-SAS bridge.

a. Create the storage zones:

    zone name STOR_zone-name vsan vsanid

b. Add storage ports to the zone:

    member STOR_zone-name

c. Activate the zone set:

    zoneset activate name STOR_zonenameesetname vsan vsanid
Example

```plaintext
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn 20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn 20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn 20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn 20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/25 swwn 20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn 20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn 20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn 20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn 20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. Create an FCVI zone set and add the FCVI ports to it:
   These steps only need to be performed on one switch in the fabric.
   a. Create the FCVI zone set:
      ```
      zoneset name FCVI_zonesetname vsan vsanid
      ```
   b. Add FCVI zones to the zone set:
      ```
      member FCVI_zonename
      ```
   c. Activate the zone set:
      ```
      zoneset activate name FCVI_zonesetname vsan vsanid
      ```

Example

```plaintext
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_20_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_20_29
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. Verify the zoning:
   ```
   show zone
   ```

7. Repeat the previous steps on the second FC switch fabric.

Ensuring the FC switch configuration is saved

You must make sure the FC switch configuration is saved to the startup config on all switches.

Step

1. Issue the following command on both FC switch fabrics:
   ```
   copy running-config startup-config
   ```
Installing FC-to-SAS bridges and SAS disk shelves

You install and cable ATTO FibreBridge bridges and SAS disk shelves when adding new storage to the configuration.

About this task

For systems received from the factory, the FC-to-SAS bridges are preconfigured and do not require additional configuration.

This procedure is written with the assumption that you are using the recommended bridge management interfaces: the ATTO ExpressNAV GUI and ATTO QuickNAV utility.

You use the ATTO ExpressNAV GUI to configure and manage a bridge, and to update the bridge firmware. You use the ATTO QuickNAV utility to configure the bridge Ethernet management 1 port.

You can use other management interfaces instead, if needed, such as a serial port or Telnet to configure and manage a bridge and to configure the Ethernet management 1 port, and FTP to update the bridge firmware.

This procedure uses the following workflow:

Example

```
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# copy running-config startup-config
```
Steps

1. In-band management of the FC-to-SAS bridges on page 152
2. Preparing for the installation on page 152
3. Installing the FC-to-SAS bridge and SAS shelves on page 153
4. Securing or unsecuring the FibreBridge bridge on page 163

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.

Preparing for the installation

When you are preparing to install the bridges as part of your new MetroCluster system, you must ensure that your system meets certain requirements, including meeting setup and configuration requirements for the bridges. Other requirements include downloading the necessary documents, the ATTO QuickNAV utility, and the bridge firmware.

Before you begin

• Your system must already be installed in a rack if it was not shipped in a system cabinet.
• Your configuration must be using supported hardware models and software versions.
  
  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.
• Each FC switch must have one FC port available for one bridge to connect to it.
• You must have familiarized yourself with how to handle SAS cables and the considerations and best practices for installing and cabling disk shelves.
  The Installation and Service Guide for your disk shelf model describes the considerations and best practices.
  
  NetApp Documentation: Disk Shelves
• The computer you are using to set up the bridges must be running an ATTO-supported web browser to use the ATTO ExpressNAV GUI.
  The ATTO Product Release Notes have an up-to-date list of supported web browsers. You can access this document from the ATTO web site as described in the following steps.

Steps

1. Download the Installation and Service Guide for your disk shelf model:
  
  NetApp Documentation: Disk Shelves
2. Access the ATTO web site using the link provided for your FibreBridge model and download the manual and the QuickNAV utility.
3. Gather the hardware and information needed to use the recommended bridge management interfaces, the ATTO ExpressNA V GUI, and the ATTO QuickNA V utility:

   a. Determine a non-default user name and password (for accessing the bridges).
      You should change the default user name and password.

   b. If configuring for IP management of the bridges, you need the shielded Ethernet cable provided with the bridges (which connects from the bridge Ethernet management 1 port to your network).

   c. If configuring for IP management of the bridges, you need 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 QuickNA V scan for bridges to fail.

Installing the FC-to-SAS bridge and SAS shelves

After ensuring that the system meets all of the requirements in the “Preparing for the installation” section, you can install your new system.

About this task

- The disk and shelf configuration at both sites should be identical.
  If a non-mirrored aggregate is used, the disk and shelf configuration at each site might be different.

  **Note:** All disks in the disaster recovery group must use the same type of connection and be visible to all of the nodes within the disaster recovery group, regardless of the disks being used for mirrored or non-mirrored aggregate.

- The system connectivity requirements for maximum distances for disk shelves, FC switches, and backup tape devices using 50-micron, multimode fiber-optic cables, also apply to FibreBridge bridges.

  **NetApp Hardware Universe**

- A mix of IOM12 modules and IOM6/IOM3 modules is not supported within the same storage stack.

  **Note:** In-band ACP is supported without additional cabling in the following shelves and FibreBridge 7500N or 7600N bridge:

  - IOM12 (DS460C) behind a 7500N or 7600N bridge with ONTAP 9.2 and later
  - IOM12 (DS212C and DS224C) behind a 7500N or 7600N bridge with ONTAP 9.1 and later

  **Note:** SAS shelves in MetroCluster configurations do not support ACP cabling.
Steps

1. Enabling IP port access on the FibreBridge 7600N bridge if necessary on page 154
2. Configuring the FC-to-SAS bridges on page 155
3. Cabling disk shelves to the bridges on page 158
4. Verifying bridge connectivity and cabling the bridge FC ports on page 162

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:
   
   ```
   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:

   ```
   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.
Configuring the FC-to-SAS bridges

Before cabling your model of the FC-to-SAS bridges, you must configure the settings in the FibreBridge software.

**Before you begin**

You should decide whether you will be using in-band management of the bridges.

**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 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.

2. 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.

3. 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.

4. Configure the bridge.
   
   You should make note of the user name and password that you designate.

   **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.
   
      In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than via IP access.
   
      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 mp1 ip-address
set ipsubnetmask mp1 subnet-mask
set ipgateway mp1 x.x.x.x
set ipdhcp mp1 disabled
set ethearnetspeed 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:
   ```bash
   set bridgename bridgename
   ```

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

   ```bash
   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.

5. 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:

      ```bash
      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

Example
The following example shows the disabling of FC port 2:

```
FCPortDisable 2
Fibre Channel Port 2 has been disabled.
```

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.

Example
If only SAS port A is used, then SAS ports B, C, and D must be disabled. The following example shows the disabling of SAS port B. You must similarly disable SAS ports C and D:

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

6. Save the bridge's configuration and secure access to 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 and configuring for in-band management, 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`
7. After completing MetroCluster configuration, use the `flashimages` command to check your version of FibreBridge firmware and, if the bridges are not using the latest supported version, update the firmware on all bridges in the configuration.

MetroCluster Service Guide

Related concepts

In-band management of the FC-to-SAS bridges on page 152

Cabling disk shelves to the bridges

You must use the correct FC-to-SAS bridges for cabling your disk shelves.

Choices

- Cabling a FibreBridge 7600N or 7500N bridge with disk shelves using IOM12 modules on page 158
- Cabling a FibreBridge 7600N or 7500N bridge with shelves using IOM6 or IOM3 modules on page 159
- Cabling a FibreBridge 6500N bridge with disk shelves using IOM6 or IOM3 modules on page 161

Cabling a FibreBridge 7600N or 7500N bridge with disk shelves using IOM12 modules

After configuring the bridge, you can start cabling your new system.

About this task

For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

Steps

1. Daisy-chain the disk shelves in each stack:
   a. Beginning with the logical first shelf in the stack, connect IOM A port 3 to the next shelf's IOM A port 1 until each IOM A in the stack is connected.
   b. Repeat the previous substep for IOM B.
   c. Repeat the previous substeps for each stack.

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

2. Power on the disk shelves, and then set the shelf IDs.
   a. You must power-cycle each disk shelf.
   b. Shelf IDs must be unique for each SAS disk shelf within the entire MetroCluster configuration (including both sites).

3. Cable disk shelves to the FibreBridge bridges.
   a. For the first stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and cable IOM B of the last shelf to SAS port A on FibreBridge B.
   b. For additional shelf stacks, repeat the previous step using the next available SAS port on the FibreBridge bridges, using port B for the second stack, port C for the third stack, and port D for the fourth stack.
c. During cabling, attach the stacks based on IOM12 and IOM3/IOM6 modules to the same bridge as long as they are connected to separate SAS ports.

   **Note:** Each stack can use different models of IOM, but all disk shelves within a stack must use the same model.

The following illustration shows disk shelves connected to a pair of FibreBridge 7600N or 7500N bridges:

---

**Cabling a FibreBridge 7600N or 7500N bridge with shelves using IOM6 or IOM3 modules**

After configuring the bridge, you can start cabling your new system. The FibreBridge 7600N or 7500N bridge uses mini-SAS connectors and supports shelves that use IOM6 or IOM3 modules.

**About this task**

IOM3 modules are not supported with FibreBridge 7600N bridges.

For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

**Steps**

1. Daisy-chain the shelves in each stack.
a. For the first stack of shelves, cable IOM A square port of the first shelf to SAS port A on FibreBridge A.

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

The *Installation and Service Guide* for your shelf model provides detailed information about daisy-chaining shelves.

*SAS Disk Shelves Installation and Service Guide for DS4243, DS2246, DS4486, and DS4246*

The following illustration shows a set of bridges cabled to a stack of shelves:

![Diagram of bridge connections]

2. For additional shelf stacks, repeat the previous steps using the next available SAS port on the FibreBridge bridges, using port B for a second stack, port C for a third stack, and port D for a fourth stack.

The following illustration shows four stacks connected to a pair of FibreBridge 7600N or 7500N bridges.
Cabling a FibreBridge 6500N bridge with disk shelves using IOM6 or IOM3 modules

After configuring the bridge, you can start cabling your new system. The FibreBridge 6500N bridge uses QSFP connectors.

About this task

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).

The FibreBridge 6500N bridge does not support disk shelves that use IOM12.

Steps

1. Daisy-chain the disk shelves in each stack.
   For information about daisy-chaining disk shelves, see the Installation and Service Guide for your disk shelf model.

2. For each stack of disk shelves, cable the IOM A square port of the first shelf to the SAS port A on FibreBridge A.

3. For each stack of disk shelves, cable the IOM B circle port of the last shelf to the SAS port A on FibreBridge B.
   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.

Example

Note: The SAS port B bridge is disabled.

The following illustration shows a set of bridges cabled to a stack of four disk shelves:
Verifying bridge connectivity and cabling the bridge FC ports

You should verify that each bridge can detect all of the disk drives, and then cable each bridge to the local FC switches.

Steps

1. Verify that each bridge can detect all of the disk drives and disk shelves it is connected to:

<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 homepage of the bridge for which you entered the IP address, 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 of the bridge appears with a menu to the left.</td>
</tr>
<tr>
<td></td>
<td>c. Click Advanced.</td>
</tr>
<tr>
<td></td>
<td>d. View the connected devices by using the <code>sastargets</code> command, and then click Submit.</td>
</tr>
</tbody>
</table>

Serial port connection

View the connected devices:

`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>3QP1CLE3000009940UHJV</td>
</tr>
<tr>
<td>1</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1ELF6000009940V1BV</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>3QP1EWMF00009940U1X5</td>
</tr>
</tbody>
</table>
Note: If the text response truncated appears at the beginning of the output, you can use Telnet to connect to the bridge and enter the same command to see all of the output.

2. Verify that the command output shows that the bridge is connected to all disks and disk shelves in the stack that it is supposed to be connected to.

<table>
<thead>
<tr>
<th>If the output is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Repeat <em>Step 1</em> on page 162 for each remaining bridge.</td>
</tr>
</tbody>
</table>
| Not correct        | a. Check for loose SAS cables or correct the SAS cabling by repeating the cabling.  
                     Cabling disk shelves to the bridges on page 158  
                     b. Repeat *Step 1* on page 162. |

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

Attention: The second FC port connection on the FibreBridge 7500N bridge should not be cabled until zoning has been completed.

See the port assignments for your version of ONTAP.

4. Repeat the previous step on the bridges at the partner site.

Related concepts
Port assignments for FC switches when using ONTAP 9.1 and later on page 52  
Port assignments for FC switches when using ONTAP 9.0 on page 37

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:
The following command unsecures bridge_A_1:

```shell
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:

```shell
storage bridge run-cli -bridge bridge-name -command saveconfiguration
```

**Example**

The following command secures bridge_A_1:

```shell
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command saveconfiguration
```

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

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

**Example**

The following command secures bridge_A_1:

```shell
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
```
Configuring hardware for sharing a Brocade 6510 FC fabric during transition

If your 7-Mode fabric MetroCluster configuration uses Brocade 6510 switches, you can share the existing switch fabrics with the new clustered MetroCluster configuration. Shared switch fabrics means the new MetroCluster configuration does not require a new, separate switch fabric. This temporary configuration is only supported with the Brocade 6510 switch for transition purposes.

Before you begin

- The 7-Mode fabric MetroCluster must be using Brocade 6510 switches. If the MetroCluster configuration is currently not using Brocade 6510 switches, the switches must be upgraded to Brocade 6510 prior to using this procedure.

- The 7-Mode fabric MetroCluster configuration must be using SAS storage shelves only. If the existing configuration includes FC storage shelves (such as the DS14mk4 FC), FC switch fabric sharing is not supported.

- The SFPs on the switch ports used by the new, clustered MetroCluster configuration must support 16-Gbps rates. The existing 7-Mode fabric MetroCluster can remain connected to ports using 8-Gbps or 16-Gbps SFPs.

- On each of the four Brocade 6510 switches, ports 24 through 45 must be available to connect the ports of the new MetroCluster components.

- You should verify that the existing Inter-Switch Links (ISLs) are on ports 46 and 47.

- The Brocade 6510 switches must be running a FOS firmware version that is supported on both the 7-Mode fabric MetroCluster and clustered ONTAP MetroCluster configuration.

After you finish

After sharing the fabric and completing the MetroCluster configuration, you can transition data from the 7-Mode fabric MetroCluster configuration.

After transitioning the data, you can remove the 7-Mode fabric MetroCluster cabling and, if desired, move the clustered ONTAP MetroCluster cabling to the lower-numbered ports previously used for the 7-Mode MetroCluster cabling. The ports are shown in the section "Reviewing FC switch port assignments for a four node MetroCluster." You must adjust the zoning for the rearranged ports.

Port assignments for FC switches when using ONTAP 9.1 and later on page 52

Steps

1. Reviewing Brocade license requirements on page 166
2. Racking the hardware components on page 166
3. Cabling the new MetroCluster controllers to the existing FC fabrics on page 167
4. Configuring switch fabrics sharing between the 7-Mode and clustered MetroCluster configuration on page 168

Related information

Copy-based transition
Reviewing Brocade license requirements

You need certain licenses for the switches in a MetroCluster configuration. You must install these licenses on all four switches.

The MetroCluster configuration has the following Brocade license requirements:

- Trunking license for systems using more than one ISL, as recommended.
- Extended Fabric license (for ISL distances over 6 km)
- Enterprise license for sites with more than one ISL and an ISL distance greater than 6 km
  The Enterprise license includes Brocade Network Advisor and all licenses except for additional port licenses.

You can verify that the licenses are installed by using the `licenseshow` command. If you do not have these licenses, you should contact your sales representative before proceeding.

Racking the hardware components

If you have not received the equipment already installed in cabinets, you must rack the components.

About this task

This task must be performed on both MetroCluster sites.

Steps

1. Plan out the positioning of the MetroCluster components.
   The rack space depends on the platform model of the controller modules, the switch types, and the number of disk shelf stacks in your configuration.

2. Properly ground yourself.

3. Install the controller modules in the rack or cabinet.

4. Install the FC switches in the rack or cabinet.

5. Install the disk shelves, power them on, and then set the shelf IDs.

   - You must power-cycle each disk shelf.
   - Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (including both sites).

6. Install each FC-to-SAS bridge:
   a. Secure the “L” brackets on the front of the bridge to the front of the rack (flush-mount) with the four screws.
      The openings in the bridge “L” brackets are compliant with rack standard ETA-310-X for 19-inch (482.6 mm) racks.
      The ATTO FibreBridge Installation and Operation Manual for your bridge model contains more information and an illustration of the installation.
**Note:** For adequate port space access and FRU serviceability, you must leave 1U space below the bridge pair and cover this space with a tool-less blanking panel.

b. Connect each bridge to a power source that provides a proper ground.

c. Power on each bridge.

**Note:** For maximum resiliency, bridges that are attached to the same stack of disk shelves must be connected to different power sources.

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

### Cabling the new MetroCluster controllers to the existing FC fabrics

On each controller in the clustered ONTAP MetroCluster configuration, the FC-VI adapter and HBAs must be cabled to specific ports on the existing FC switches.

**Steps**

1. Cable the FC-VI and HBA ports according to the following table:

<table>
<thead>
<tr>
<th>Site A</th>
<th>Site B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connect this Site A component and port...</strong></td>
<td><strong>Connect this Site B component and port...</strong></td>
</tr>
<tr>
<td>controller_A_1 FC-VI port 1</td>
<td>controller_B_1 FC-VI port 1</td>
</tr>
<tr>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>controller_A_1 HBA port 1</td>
<td>controller_B_1 HBA port 1</td>
</tr>
<tr>
<td>33</td>
<td>33</td>
</tr>
<tr>
<td>controller_A_1 HBA port 2</td>
<td>controller_B_1 HBA port 2</td>
</tr>
<tr>
<td>34</td>
<td>34</td>
</tr>
<tr>
<td>controller_A_2 FC-VI port 1</td>
<td>controller_B_1 FC-VI port 1</td>
</tr>
<tr>
<td>35</td>
<td>35</td>
</tr>
<tr>
<td>controller_A_2 HBA 1</td>
<td>controller_B_2 HBA 1</td>
</tr>
<tr>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>controller_A_2 HBA 2</td>
<td>controller_B_2 HBA 2</td>
</tr>
<tr>
<td>37</td>
<td>37</td>
</tr>
</tbody>
</table>

2. Cable each FC-SAS bridge in the first switch fabric to the FC switches.

   The number of bridges varies depending on the number of SAS storage stacks.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Site B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cable this site A bridge...</strong></td>
<td><strong>Cable this Site B bridge...</strong></td>
</tr>
<tr>
<td>bridge_A_1_38</td>
<td>bridge_B_1_38</td>
</tr>
<tr>
<td>38</td>
<td>38</td>
</tr>
<tr>
<td>bridge_A_1_39</td>
<td>bridge_B_1_39</td>
</tr>
<tr>
<td>39</td>
<td>39</td>
</tr>
</tbody>
</table>

3. Cable each bridge in the second switch fabric to the FC switches.

   The number of bridges varies depending on the number of SAS storage stacks.
Configuring switch fabrics sharing between the 7-Mode and clustered MetroCluster configuration

To share switch fabrics between the existing 7-Mode fabric MetroCluster and the new MetroCluster configuration, you must set up specific zoning and other settings that are different than an unshared configuration.

About this task

This task must be performed on both switch fabrics, one at a time.

Disabling one of the switch fabrics

You must disable one of the switch fabrics so you can modify its configuration. After you complete the configuration and reenable the switch fabric, you will repeat the process on the other fabric.

Before you begin

You must have run the fmc_dc utility on the existing 7-Mode fabric MetroCluster configuration and resolved any issues prior to beginning the configuration process.

About this task

To ensure continued operation of the MetroCluster configuration, you must not disable the second fabric while the first fabric is disabled.

Steps

1. Disable each of the switches in the fabric:

   `switchCfgPersistentDisable`

   If this command is not available, use the `switchDisable` command.

   **Example**

   The following example shows the command issued on FC_switch_A_1:

   ```shell
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

   The following example shows the command issued on FC_switch_B_1:

   ```shell
   FC_switch_B_1:admin> switchCfgPersistentDisable
   ```

2. Ensure that the 7-Mode MetroCluster configuration is functioning correctly using the redundant fabric:

   a. Confirm that controller failover is healthy:
### cf status

**Example**

```bash
node_A> cf status
Controller Failover enabled, node_A is up.
VIA Interconnect is up (link 0 down, link 1 up).
```

b. Confirm that disks are visible:

**storage show disk -p**

**Example**

```bash
node_A> storage show disk -p
```

<table>
<thead>
<tr>
<th>PRIMARY</th>
<th>PORT</th>
<th>SECONDARY</th>
<th>PORT</th>
<th>SHELF</th>
<th>BAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade-6510-2K0GG:5.126L27</td>
<td>B</td>
<td></td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Brocade-6510-2K0GG:5.126L28</td>
<td>B</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Brocade-6510-2K0GG:5.126L29</td>
<td>B</td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Brocade-6510-2K0GG:5.126L30</td>
<td>B</td>
<td></td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Brocade-6510-2K0GG:5.126L31</td>
<td>B</td>
<td></td>
<td>1</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

...  

**Deleting TI zoning and configuring IOD settings**

You must delete the existing TI zoning and reconfigure in-order-delivery (IOD) settings on the switch fabric.

**Steps**

1. Identify the TI zones that are configured on the fabric:

   **zone --show**

   **Example**

   The following example shows the zone FCVI_TI_FAB_2.

   ```bash
   Brocade-6510:admin> zone --show
   Defined TI zone configuration:
   TI Zone Name:   FCVI_TI_FAB_2
   Port List:      1,0; 1,3; 2,0; 2,3
   configured Status: Activated / Failover-Disabled
   Enabled Status: Activated / Failover-Disabled
   ```
2. Delete the TI zones:

\[ \text{zone --delete zone-name} \]

**Example**
The following example shows the deletion of zone FCVI_TI_FAB_2.

Brocade-6510:admin> zone --delete FCVI_TI_FAB_2

3. Confirm that the zones have been deleted:

\[ \text{zone --show} \]

**Example**
The output should be similar to the following:

Brocade-6510:admin> zone --show

  Defined TI zone configuration:
  no TI zone configuration defined

4. Save the configuration:

\[ \text{cfgsave} \]

5. Enable in-order-delivery:

\[ \text{iodset} \]

6. Select Advanced Performance Tuning (APT) policy 1, the Port Based Routing Policy:

\[ \text{aptpolicy 1} \]

7. Disable Dynamic Load Sharing (DLS):

\[ \text{dlsreset} \]

8. Verify the IOD settings using the following commands:

\[ \text{iodshow} \]
\[ \text{aptpolicy} \]
\[ \text{dlsshow} \]

**Example**
The output should be similar to the following:

Brocade-6510:admin> iodshow

  IOD is set

Brocade-6510:admin> aptpolicy
  Current Policy: 1

  3 : Default Policy
  1: Port Based Routing Policy
  2: Device Based Routing Policy (FICON support only)
  3: Exchange Based Routing Policy

Brocade-6510:admin> dlsshow

  DLS is not set
Ensuring ISLs are in the same port group and configuring zoning

You must make sure that the Inter-Switch Links (ISLs) are in the same port group and configure zoning for the MetroCluster configurations to successfully share the switch fabrics.

Steps

1. If the ISLs are not in the same port group, move one of the ISL ports to the same port group as the other one.
   
   You can use any available port except 32 through 45, which are used by the new MetroCluster configuration. The recommended ISL ports are 46 and 47.

2. Follow the steps in the Configuring zoning on a Brocade FC switch section to enable trunking and the QoS zone.

   Configuring zoning on Brocade FC switches on page 95

   The port numbers when sharing fabrics are different than those shown in the section. When sharing, use ports 46 and 47 for the ISL ports. If you moved your ISL ports, you need to use the procedure in the Configuring the E-ports (ISL ports) on a Brocade FC switch section to configure the ports.

   Configuring the E-ports (ISL ports) on a Brocade FC switch on page 82

3. Follow the steps in the Configuring the non-E ports on the Brocade switch section to configure the non-E ports.

   Configuring the non-E ports on the Brocade switch on page 93

4. Do not delete the zones or zone sets that already exist in the backend switches (for the 7-Mode fabric MetroCluster) except the Traffic Isolation (TI) zones in Step 3.

5. Follow the steps in the Configuring the E-ports (ISL ports) on a Brocade FC switch section to add the zones required by the new MetroCluster to the existing zone sets.

   Configuring the E-ports (ISL ports) on a Brocade FC switch on page 82

Example

The following example shows the commands and system output for creating the zones:

```
Brocade-6510-2K0GG:admin> zonecreate "QOSH2_FCVI_1", "2,32; 2,35; 1,32; 1,35"
Brocade-6510-2K0GG:admin> zonecreate "STOR_A_2_47", "2,33; 2,34; 2,36; 2,37; 1,33; 1,34; 1,36; 1,37; 1,47"
Brocade-6510-2K0GG:admin> zonecreate "STOR_B_2_47", "2,33; 2,34; 2,36; 2,37; 1,33; 1,34; 1,36; 1,37; 2,47"
Brocade-6510-2K0GG:admin> cfgadd config_1_FAB2, "QOSH2_FCVI_1; STOR_A_2_47; STOR_B_2_47"
Brocade-6510-2K0GG:admin> cfgenable "config_1_FAB2"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the current configuration selected. If the update includes changes to one or more traffic isolation zones, the update may result in localized disruption to traffic on ports associated with the traffic isolation zone changes
Do you want to enable 'config_1_FAB2' configuration (yes, y, no, n): [no] yes
Brocade-6510-2K0GG:admin> cfgsave
```
You are about to save the Defined zoning configuration. This action will only save the changes on Defined configuration. Do you want to save the Defined zoning configuration only? (yes, y, no, n): [no] yes
Nothing changed: nothing to save, returning ...
Brocade-6510-2K0GG:admin>

Reenabling the switch fabric and verify operation

You must enable the FC switch fabric and ensure that the switches and devices are operating correctly.

Steps

1. Enable the switches:

   `switchCfgPersistentEnable`

   If this command is not available, the switch should be in the enabled state after the `fastBoot` command is issued.

   Example

   The following example shows the command issued on FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchCfgPersistentEnable
   ```

   The following example shows the command issued on FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchCfgPersistentEnable
   ```

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

   `switchShow`

   Example

   The following example shows the command issued on FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchShow
   ```

   The following example shows the command issued on FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchShow
   ```

3. Run the `fmc_dc` utility to ensure that the 7-Mode fabric MetroCluster is functioning correctly.

   You can ignore errors related to Traffic Isolation (TI) zoning and trunking.

4. Repeat the tasks for the second switch fabric.
**Configuring the MetroCluster software in ONTAP**

You must set up each node in the MetroCluster configuration in ONTAP, including the node-level configurations and the configuration of the nodes into two sites. You must also implement the MetroCluster relationship between the two sites. The steps for systems with native disk shelves are slightly different from those for systems with array LUNs.

**Steps**

1. Gathering required information on page 174
2. Similarities and differences between standard cluster and MetroCluster configurations on page 179
3. Restoring system defaults and configuring the HBA type on a previously used controller module on page 179
4. Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems on page 180
5. Verifying disk assignment in Maintenance mode in an eight-node or a four-node configuration on page 182
6. Verifying disk assignment in Maintenance mode in a two-node configuration on page 188
7. Verifying and configuring the HA state of components in Maintenance mode on page 190
8. Setting up ONTAP on page 191
9. Configuring the clusters into a MetroCluster configuration on page 196
10. Checking for MetroCluster configuration errors with Config Advisor on page 216
11. Verifying local HA operation on page 216
12. Verifying switchover, healing, and switchback on page 218
13. Installing the MetroCluster Tiebreaker software on page 218
14. Protecting configuration backup files on page 218

Gathering required information

You need to gather the required IP addresses for the controller modules before you begin the configuration process.

IP network information worksheet for site A

You must obtain IP addresses and other network information for the first MetroCluster site (site A) from your network administrator before you configure the system.

Site A switch information (switched clusters)

When you cable the system, you need a host name and management IP address for each cluster switch. This information is not needed if you are using a two-node switchless cluster or have a two-node MetroCluster configuration (one node at each site).

<table>
<thead>
<tr>
<th>Cluster switch</th>
<th>Host name</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interconnect 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interconnect 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Site A cluster creation information

When you first create the cluster, you need the following information:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td></td>
</tr>
<tr>
<td>Example used in this guide: site_A</td>
<td></td>
</tr>
<tr>
<td>DNS domain</td>
<td></td>
</tr>
<tr>
<td>DNS name servers</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Administrator password</td>
<td></td>
</tr>
</tbody>
</table>

Site A node information

For each node in the cluster, you need a management IP address, a network mask, and a default gateway.
### Site A LIFs and ports for cluster peering

For each node in the cluster, you need the IP addresses of two intercluster LIFs, including a network mask and a default gateway. The intercluster LIFs are used to peer the clusters.

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IP address of intercluster LIF</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 IC LIF 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 1 IC LIF 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2 IC LIF 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2 IC LIF 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Site A time server information

You must synchronize the time, which requires one or more NTP time servers.

<table>
<thead>
<tr>
<th>Node</th>
<th>Host name</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP server 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Site A AutoSupport information

You must configure AutoSupport on each node, which requires the following information:
### Site A SP information

You must enable access to the Service Processor (SP) of each node for troubleshooting and maintenance, which requires the following network information for each node:

<table>
<thead>
<tr>
<th>Node</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not required for two-node MetroCluster configurations (one node at each site).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IP network information worksheet for site B

You must obtain IP addresses and other network information for the second MetroCluster site (site B) from your network administrator before you configure the system.

### Site B switch information (switched clusters)

When you cable the system, you need a host name and management IP address for each cluster switch. This information is not needed if you are using a two-node switchless cluster or you have a two-node MetroCluster configuration (one node at each site).

<table>
<thead>
<tr>
<th>Cluster switch</th>
<th>Host name</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interconnect 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interconnect 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Site B cluster creation information

When you first create the cluster, you need the following information:
### Type of information

<table>
<thead>
<tr>
<th>Your values</th>
</tr>
</thead>
</table>
| Cluster name
   Example used in this guide: site_B |
| DNS domain |
| DNS name servers |
| Location |
| Administrator password |

### Site B node information

For each node in the cluster, you need a management IP address, a network mask, and a default gateway.

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example used in this guide: controller_B_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Not required for two-node MetroCluster configurations (one node at each site).
   Example used in this guide: controller_B_2 |

### Site B LIFs and ports for cluster peering

For each node in the cluster, you need the IP addresses of two intercluster LIFs, including a network mask and a default gateway. The intercluster LIFs are used to peer the clusters.

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IP address of intercluster LIF</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 IC LIF 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 1 IC LIF 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Node 2 IC LIF 1
   Not required for two-node MetroCluster configurations (one node at each site). |
### Node 2 IC LIF 2
Not required for two-node MetroCluster configurations (one node at each site).

### Site B time server information
You must synchronize the time, which requires one or more NTP time servers.

<table>
<thead>
<tr>
<th>Node</th>
<th>Host name</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP server 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Site B AutoSupport information
You must configure AutoSupport on each node, which requires the following information:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>From email address</td>
<td></td>
</tr>
<tr>
<td>Mail hosts</td>
<td>IP addresses or names</td>
</tr>
<tr>
<td>Transport protocol</td>
<td>HTTP, HTTPS, or SMTP</td>
</tr>
<tr>
<td>Proxy server</td>
<td></td>
</tr>
<tr>
<td>Recipient email addresses or distribution lists</td>
<td>Full-length messages</td>
</tr>
<tr>
<td></td>
<td>Concise messages</td>
</tr>
<tr>
<td></td>
<td>Partners</td>
</tr>
</tbody>
</table>

### Site B SP information
You must enable access to the Service Processor (SP) of each node for troubleshooting and maintenance, which requires the following network information for each node:

<table>
<thead>
<tr>
<th>Node</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 (controller_B_1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2 (controller_B_2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not required for two-node MetroCluster configurations (one node at each site).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Similarities and differences between standard cluster and MetroCluster configurations

The configuration of the nodes in each cluster in a MetroCluster configuration is similar to that of nodes in a standard cluster.

The MetroCluster configuration is built on two standard clusters. Physically, the configuration must be symmetrical, with each node having the same hardware configuration, and all of the MetroCluster components must be cabled and configured. However, the basic software configuration for nodes in a MetroCluster configuration is the same as that for nodes in a standard cluster.

<table>
<thead>
<tr>
<th>Configuration step</th>
<th>Standard cluster configuration</th>
<th>MetroCluster configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure management, cluster, and data LIFs on each node.</td>
<td>Same in both types of clusters</td>
<td></td>
</tr>
<tr>
<td>Configure the root aggregate.</td>
<td>Same in both types of clusters</td>
<td></td>
</tr>
<tr>
<td>Configure nodes in the cluster as HA pairs</td>
<td>Same in both types of clusters</td>
<td></td>
</tr>
<tr>
<td>Set up the cluster on one node in the cluster.</td>
<td>Same in both types of clusters</td>
<td></td>
</tr>
<tr>
<td>Join the other node to the cluster.</td>
<td>Same in both types of clusters</td>
<td></td>
</tr>
<tr>
<td>Create a mirrored root aggregate.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Peer the clusters.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Enable the MetroCluster configuration.</td>
<td>Does not apply</td>
<td>Required</td>
</tr>
</tbody>
</table>

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:
   
   ```shell
   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...**

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA FC</td>
<td><code>ucadmin modify -m fc -t initiator adapter_name</code></td>
</tr>
<tr>
<td>CNA Ethernet</td>
<td><code>ucadmin modify -mode cna adapter_name</code></td>
</tr>
<tr>
<td>FC target</td>
<td><code>fcadmin config -t target adapter_name</code></td>
</tr>
</tbody>
</table>
If you have this type of HBA and desired mode...

<table>
<thead>
<tr>
<th>FC initiator</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fcadmin config -t initiator adapter_name</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>If you have this type of HBA...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA</td>
<td>ucadmin show</td>
</tr>
<tr>
<td>FC</td>
<td>fcadmin show</td>
</tr>
</tbody>
</table>

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:

   1) Normal Boot.
   2) Boot without /etc/rc.
   3) Change password.
   4) Clean configuration and initialize all disks.
   5) Maintenance mode boot.
   6) Update flash from backup config.
   7) Install new software first.
   8) Reboot node.
   9) Configure Advanced Drive Partitioning.

   Selection (1-9)? wipeconfig

   This option deletes critical system configuration, including cluster membership.

   Warning: do not run this option on a HA node that has been taken over.

   Are you sure you want to continue?: yes

   Rebooting to finish wipeconfig request.

Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems

If you are using the X1132A-R6 quad-port card on a FAS8020 system, you can enter Maintenance mode to configure the 1a and 1b ports for FC-VI and initiator usage. This is not required on
MetroCluster systems received from the factory, in which the ports are set appropriately for your configuration.

**About this task**

This task must be performed in Maintenance mode.

**Steps**

1. Disable the ports:
   
   ```
   storage disable adapter 1a
   ```
   
   ```
   storage disable adapter 1b
   ```
   
   **Example**
   
   ```
   *> storage disable adapter 1a
   Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]:
   Offlining Fibre Channel adapter 1a.
   Host adapter 1a disable succeeded
   Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre
   Channel adapter 1a is now offline.
   *> storage disable adapter 1b
   Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]:
   Offlining Fibre Channel adapter 1b.
   Host adapter 1b disable succeeded
   Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre
   Channel adapter 1b is now offline.
   *
   ```
   
   2. Verify that the ports are disabled:
      
      ```
      uadmin show
      ```
      
      **Example**
      
      ```
      *> uadmin show
      Current  Current    Pending  Pending    Admin
      Adapter  Mode     Type       Mode     Type       Status
      -------  -------  ---------  -------  ---------  -------
      ...     ...       ...       ...       ...
      1a     fc       initiator  -        -          offline
      1b     fc       initiator  -        -          offline
      1c     fc       initiator  -        -          online
      1d     fc       initiator  -        -          online
      ```
      
   3. Set the a and b ports to FC-VI mode:
      
      ```
      uadmin modify -adapter 1a -type fcvi
      ```
      
      The command sets the mode on both ports in the port pair, 1a and 1b (even though only 1a is specified in the command).
      
      **Example**
      
      ```
      *> uadmin modify -t fcvi 1a
      Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
      changed to fcvi on adapter 1a. Reboot the controller for the changes
      to take effect.
      Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
      changed to fcvi on adapter 1b. Reboot the controller for the changes
      to take effect.
      ```
4. Confirm that the change is pending:

`ucadmin show`

**Example**

```
*> ucadmin show

<table>
<thead>
<tr>
<th>Adapter</th>
<th>Mode</th>
<th>Type</th>
<th>Pending Mode</th>
<th>Type</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>fcvi</td>
<td>offline</td>
</tr>
<tr>
<td>1b</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>fcvi</td>
<td>offline</td>
</tr>
<tr>
<td>1c</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>1d</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>
```

5. Shut down the controller, and then reboot into Maintenance mode.

6. Confirm the configuration change:

`ucadmin show local`

**Example**

```
<table>
<thead>
<tr>
<th>Node</th>
<th>Adapter</th>
<th>Mode</th>
<th>Type</th>
<th>Pending Mode</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1a</td>
<td>fc</td>
<td>fcvi</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1b</td>
<td>fc</td>
<td>fcvi</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1c</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1d</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>
6 entries were displayed.
```

**Verifying disk assignment in Maintenance mode in an eight-node or a four-node configuration**

Before fully booting the system to ONTAP, you can optionally boot to Maintenance mode and verify the disk assignment on the nodes. The disks should be assigned to create a fully symmetric active-active configuration, where each pool has an equal number of disks assigned to them.

**About this task**

New MetroCluster systems have disk assignment completed prior to shipment.

The following table shows example pool assignments for a MetroCluster configuration. Disks are assigned to pools on a per-shelf basis.
<table>
<thead>
<tr>
<th>Disk shelf (sample_shelf_name)</th>
<th>At site...</th>
<th>Belongs to...</th>
<th>And is assigned to that node's...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk shelf 1 (shelf_A_1_1)</td>
<td>Site A</td>
<td>Node A 1</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 2 (shelf_A_1_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 3 (shelf_B_1_1)</td>
<td></td>
<td>Node B 1</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 4 (shelf_B_1_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 5 (shelf_A_2_1)</td>
<td></td>
<td>Node A 2</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 6 (shelf_A_2_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 7 (shelf_B_2_1)</td>
<td></td>
<td>Node B 2</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 8 (shelf_B_2_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 1 (shelf_A_3_1)</td>
<td></td>
<td>Node A 3</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 2 (shelf_A_3_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 3 (shelf_B_3_1)</td>
<td></td>
<td>Node B 3</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 4 (shelf_B_3_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 5 (shelf_A_4_1)</td>
<td></td>
<td>Node A 4</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 6 (shelf_A_4_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 7 (shelf_B_4_1)</td>
<td></td>
<td>Node B 4</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 8 (shelf_B_4_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf (sample_shelf_name)</td>
<td>At site...</td>
<td>Belongs to...</td>
<td>And is assigned to that node's...</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
<td>---------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Disk shelf 9 (shelf_B_1_2)</td>
<td>Site B</td>
<td>Node B 1</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 10 (shelf_B_1_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 11 (shelf_A_1_2)</td>
<td></td>
<td>Node A 1</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 12 (shelf_A_1_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 13 (shelf_B_2_2)</td>
<td></td>
<td>Node B 2</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 14 (shelf_B_2_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 15 (shelf_A_2_2)</td>
<td></td>
<td>Node A 2</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 16 (shelf_A_2_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 1 (shelf_B_3_2)</td>
<td></td>
<td>Node A 3</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 2 (shelf_B_3_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 3 (shelf_A_3_2)</td>
<td></td>
<td>Node B 3</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 4 (shelf_A_3_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 5 (shelf_B_4_2)</td>
<td></td>
<td>Node A 4</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 6 (shelf_B_4_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 7 (shelf_A_4_2)</td>
<td></td>
<td>Node B 4</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 8 (shelf_A_4_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Steps**

1. Confirm the shelf assignments:
   ```
   disk show -v
   ```
2. If necessary, explicitly assign disks on the attached disk shelves to the appropriate pool by using the `disk assign` command.
   Using wildcards in the command enables you to assign all of the disks on a disk shelf with one command. You can identify the disk shelf IDs and bays for each disk with the `storage show disk -x` command.
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:

   \[ \text{disk assign --shelf local-switch-name:shelf-name.port -p pool} \]

Example

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

\[
* \text{disk assign --shelf FC_switch_A_1:1-4.shelf1 -p 0} \\
* \text{disk assign --shelf FC_switch_A_1:1-4.shelf2 -p 0} \\
* \text{disk assign --shelf FC_switch_B_1:1-4.shelf1 -p 1} \\
* \text{disk assign --shelf FC_switch_B_1:1-4.shelf2 -p 1}
\]
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:

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

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0
*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

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

\[
\text{disk assign -shelf shelf-name -p pool}
\]

**Example**

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

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0
*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

### 4. Confirm the shelf assignments:

\[
\text{storage show shelf}
\]

### 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.
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_A_1:1-4.shelf4 -p 1 -n 4
   *> disk assign -shelf FC_switch_B_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:

   \[\text{disk assign} \ -\text{disk disk-name} \ -p \text{ pool}\]

   \textbf{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:

   \[\text{disk assign} \ -\text{disk disk-name} \ -p \text{ pool}\]

   \textbf{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 0 -n 4
   > disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
   > disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4

4. Confirm the disk assignments:

\[\text{storage show disk}\]

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.

\textbf{Verifying disk assignment in Maintenance mode in a two-node configuration}

Before fully booting the system to ONTAP, you can optionally boot the system to Maintenance mode and verify the disk assignment on the nodes. The disks should be assigned to create a fully symmetric configuration with both sites owning their own disk shelves and serving data, where each node and each pool have an equal number of mirrored disks assigned to them.

\textbf{Before you begin}

The system must be in Maintenance mode.
About this task

New MetroCluster systems have disk assignment completed prior to shipment.

The following table shows example pool assignments for a MetroCluster configuration. Disks are assigned to pools on a per-shelf basis.

<table>
<thead>
<tr>
<th>Disk shelf (example name)</th>
<th>At site...</th>
<th>Belongs to...</th>
<th>And is assigned to that node's...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk shelf 1 (shelf_A_1_1)</td>
<td>Site A</td>
<td>Node A 1</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 2 (shelf_A_1_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 3 (shelf_B_1_1)</td>
<td></td>
<td>Node B 1</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 4 (shelf_B_1_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 9 (shelf_B_1_2)</td>
<td>Site B</td>
<td>Node B 1</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 10 (shelf_B_1_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 11 (shelf_A_1_2)</td>
<td></td>
<td>Node A 1</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 12 (shelf_A_1_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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>1 - 6</td>
<td>Local node's pool 0</td>
</tr>
<tr>
<td>7 - 12</td>
<td>DR partner's pool 1</td>
</tr>
</tbody>
</table>

This disk assignment pattern minimizes the effect on an aggregate if a drawer goes offline.

Steps

1. If your system was received from the factory, confirm the shelf assignments:
   `disk show -v`

2. If necessary, you can explicitly assign disks on the attached disk shelves to the appropriate pool by using the `disk assign` command.
   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. If you have not done so, boot each system into Maintenance mode.
   b. On the node on site A, systematically assign the local disk shelves to pool 0 and the remote disk shelves to pool 1:
      `disk assign -shelf disk_shelf_name -p pool`
Example
If storage controller node_A_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0
*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

c. On the node at the remote site (site B), systematically assign its local disk shelves to pool 0 and its remote disk shelves to pool 1:

```
disk assign -shelf disk_shelf_name -p pool
```

Example
If storage controller node_B_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf shelf_B_1_2 -p 0
*> disk assign -shelf shelf_B_1_4 -p 0
*> disk assign -shelf shelf_B_1_1 -p 1
*> disk assign -shelf shelf_B_1_3 -p 1
```

d. Show the disk shelf IDs and bays for each disk:

```
disk show -v
```

Verifying and configuring the HA state of components in Maintenance mode

When configuring a storage system in a MetroCluster configuration, you must make sure that the high-availability (HA) state of the controller module and chassis components is `mcc` or `mcc-2n` so that these components boot properly.

**Before you begin**
The system must be in Maintenance mode.

**About this task**
This task is not required on systems that are received from the factory.

**Steps**

1. In Maintenance mode, display the HA state of the controller module and chassis:
   ```
   ha-config show
   ```
The correct HA state depends on your MetroCluster configuration.

<table>
<thead>
<tr>
<th>Number of controllers in the MetroCluster configuration</th>
<th>HA state for all components should be...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eight- or four-node MetroCluster FC configuration</td>
<td>mcc</td>
</tr>
</tbody>
</table>
2. If the displayed system state of the controller is not correct, set the HA state for the controller module:

<table>
<thead>
<tr>
<th>Number of controllers in the MetroCluster configuration</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eight- or four-node MetroCluster FC configuration</td>
<td>ha-config modify controller mcc</td>
</tr>
<tr>
<td>Two-node MetroCluster FC configuration</td>
<td>ha-config modify controller mcc-2n</td>
</tr>
<tr>
<td>MetroCluster IP configuration</td>
<td>ha-config modify controller mccip</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Number of controllers in the MetroCluster configuration</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eight- or four-node MetroCluster FC configuration</td>
<td>ha-config modify chassis mcc</td>
</tr>
<tr>
<td>Two-node MetroCluster FC configuration</td>
<td>ha-config modify chassis mcc-2n</td>
</tr>
<tr>
<td>MetroCluster IP configuration</td>
<td>ha-config modify chassis mccip</td>
</tr>
</tbody>
</table>

4. Boot the node to ONTAP:

   boot_ontap

5. Repeat these steps on each node in the MetroCluster configuration.

### Setting up ONTAP

You must set up ONTAP on each controller module.

**Choices**

- Setting up ONTAP in a two-node MetroCluster configuration on page 191
- Setting up ONTAP in an eight-node or four-node MetroCluster configuration on page 193

### Setting up ONTAP in a two-node MetroCluster configuration

In a two-node MetroCluster configuration, on each cluster you must boot up the node, exit the Node Setup wizard, and use the Cluster Setup wizard to configure the node into a single-node cluster.

**Before you begin**

You must not have configured the Service Processor.
About this task

This task is for two-node MetroCluster configurations using native NetApp storage.

New MetroCluster systems are preconfigured; you do not need to perform these steps. However, you should configure AutoSupport.

This task must be performed on both clusters in the MetroCluster configuration.

For more general information about setting up ONTAP, see the Software Setup Guide

Steps

1. Power on the first node.

   The node boots, and then the Node Setup wizard starts on the console, informing you that AutoSupport will be enabled automatically.

   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.

   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, see: http://support.netapp.com/autosupport/

   Type yes to confirm and continue {yes}:

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

   exit

   The Node Setup might be used to configure the node's node management interface for use with the Cluster Setup wizard.

   The Node Setup wizard exits, and a login prompt appears, warning that you have not completed the setup tasks.

   Exiting the node setup wizard. Any changes you made have been saved.

   Warning: You have exited the node setup wizard before completing all of the tasks. The node is not configured. You can complete node setup by typing "node setup" in the command line interface.

   login:

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

4. Start the Cluster Setup wizard:

   cluster setup
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.

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

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

5. Create a new cluster:
   create

6. Accept the system defaults by pressing Enter, or enter your own values by typing no, and then pressing Enter.

7. Follow the prompts to complete the Cluster Setup wizard, pressing Enter to accept the default values or typing your own values and then pressing Enter.
   The default values are determined automatically based on your platform and network configuration.

8. After you complete the Cluster Setup wizard and it exits, verify that the cluster is active and the first 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:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           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.

Related information

Software setup

Setting up ONTAP in an eight-node or four-node MetroCluster configuration

After you boot each node, you are prompted to run the System Setup tool to perform basic node and cluster configuration. After configuring the cluster, you return to the ONTAP CLI to create aggregates and create the MetroCluster configuration.

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 is for eight-node or four-node MetroCluster configurations using native NetApp storage.

New MetroCluster systems are preconfigured; you do not need to perform these steps. However, you should configure the AutoSupport tool.

This task must be performed on both clusters in the MetroCluster configuration.

This procedure uses the System Setup tool. If desired, you can use the CLI cluster setup wizard instead.

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`

   **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 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 the MetroCluster configuration is performed 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 cluster_A:

```
cluster_A::> network port show
Speed (Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- ------------
node_A_1  e0a       Cluster      Cluster          up       1500  auto/1000
e0b       Cluster      Cluster          up       1500  auto/1000
e0c       Default     Default          up       1500  auto/1000
e0d       Default     Default          up       1500  auto/1000
e0e       Default     Default          up       1500  auto/1000
e0f       Default     Default          up       1500  auto/1000
e0g       Default     Default          up       1500  auto/1000
node_A_2  e0a       Cluster      Cluster          up       1500  auto/1000
e0b       Cluster      Cluster          up       1500  auto/1000
e0c       Default     Default          up       1500  auto/1000
e0d       Default     Default          up       1500  auto/1000
e0e       Default     Default          up       1500  auto/1000
e0f       Default     Default          up       1500  auto/1000
e0g       Default     Default          up       1500  auto/1000
14 entries were displayed.
```

6. If you are creating a two-node switchless cluster (a cluster without cluster interconnect switches), enable the switchless-cluster networking mode:

   a. Change to the advanced privilege level:

   ```bash
   set -privilege advanced
   ```

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

   b. Enable switchless-cluster mode:

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

   c. Return to the admin privilege level:

   ```bash
   set -privilege admin
   ```

7. Launch the System Setup tool as directed by the information that appears on the system console after the initial boot.

8. Use the System Setup tool to configure each node and create the cluster, but do not create aggregates.

   **Note:** You create mirrored aggregates in later tasks.

**After you finish**

Return to the ONTAP command-line interface and complete the MetroCluster configuration by performing the tasks that follow.
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.

Peering the clusters

The clusters in the MetroCluster configuration must be in a peer relationship so that they can communicate with each other and perform the data mirroring essential to MetroCluster disaster recovery.

Steps

1. Configuring intercluster LIFs on page 196
2. Creating a cluster peer relationship on page 200

Related concepts

Considerations when using dedicated ports on page 11
Considerations when sharing data ports on page 11

Related information

Cluster and SVM peering express configuration

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 196
• Configuring intercluster LIFs on shared data ports on page 199

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:

```
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>
<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>
</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:

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

3. Create a failover group for the dedicated ports:

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

**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
Vserver   Group          Failover Targets
--------- ---------------- --------------------------------------------
Cluster   Cluster         cluster01-01:e0a, cluster01-01:e0b,
cluster01 Default         cluster01-02:e0a, cluster01-02:e0b
cluster01
intercluster01             cluster01-01:e0c, cluster01-01:e0d,
cluster01-01:e0e, cluster01-01:e0f
```

Configuring the MetroCluster software in ONTAP | 197
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`:

```bash
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    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    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
Failover Targets:  cluster01-01:e0e, cluster01-01:e0f
cluster01-01 cluster01-01_icl02 cluster01-01:e0e   local-only      intercluster01
Failover Targets:  cluster01-02:e0e, cluster01-02:e0f
```

Related concepts

`Considerations when using dedicated ports` on page 11
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
   |
   +-----------------+----------+-----------+-----------------+----------+------+
   | Speed (Mbps)    |
   | Node   Port      | IPspace  | Broadcast Domain | Link    | MTU    | Admin/Oper |
   +-----------------+----------+-----------+-----------------+----------+------+
   | cluster01-01    |
   | e0a Cluster     | Cluster  | up         | 1500           | auto/1000|
   | e0b Cluster     | Cluster  | up         | 1500           | auto/1000|
   | e0c Default     | Default  | up         | 1500           | auto/1000|
   | e0d Default     | Default  | up         | 1500           | auto/1000|
   +-----------------+----------+-----------+-----------------+----------+------+
   | cluster01-02    |
   | e0a Cluster     | Cluster  | up         | 1500           | auto/1000|
   | e0b Cluster     | Cluster  | up         | 1500           | auto/1000|
   | e0c Default     | Default  | up         | 1500           | auto/1000|
   | e0d Default     | Default  | up         | 1500           | auto/1000|
   +-----------------+----------+-----------+-----------------+----------+------+
   ```

2. Create intercluster LIFs on the system SVM:

   `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 |
   | Server          | Admin/Oper | Address/Port | 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

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
      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
```

Related concepts

Considerations when sharing data ports on page 11

Creating a cluster peer relationship

You must create the cluster peer relationship between the MetroCluster clusters.

Creating a cluster peer relationship

You can use the `cluster peer create` command to create a peer relationship between a local and remote cluster. After the peer relationship has been created, you can run `cluster peer create` on the remote cluster to authenticate it to the local cluster.

Before you begin

- You must have created intercluster LIFs on every node in the clusters that are being peered.
- The clusters must be running ONTAP 9.3 or later.

About this task

Steps

1. On the destination cluster, create a peer relationship with the source cluster:

   `cluster peer create -generate-passphrase -offer-expiration MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs peer_LIF_IPs -ipspace ipspace`

   If you specify both `-generate-passphrase` and `-peer-addrs`, only the cluster whose intercluster LIFs are specified in `-peer-addrs` can use the generated password.

   You can ignore the `-ipspace` option if you are not using a custom IPspace. For complete command syntax, see the man page.

Example

The following example creates a cluster peer relationship on an unspecified remote cluster:

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration 2days
```
2. On source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace
```

For complete command syntax, see the man page.

**Example**

The following example authenticates the local cluster to the remote cluster at intercluster LIF IP addresses 192.140.112.101 and 192.140.112.102:

```
cluster01::> cluster peer create -peer-addrs 192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.
To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

Enter the passphrase for the peer relationship when prompted.

3. Verify that the cluster peer relationship was created:

```
cluster peer show -instance
```

**Example**

```
cluster01::> cluster peer show -instance
```

```
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.140.112.101, 192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.140.112.101, 192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default
```

4. Check the connectivity and status of the nodes in the peer relationship:

```
cluster peer health show
```

**Example**

```
cluster01::> cluster peer health show
```

```
Node       cluster-Name                Node-Name       Ping-Status       RDB-Health Cluster-Health
Avail...
Creating a cluster peer relationship (ONTAP 9.2 and earlier)

You can use the `cluster peer create` command to initiate a request for a peering relationship between a local and remote cluster. After the peer relationship has been requested by the local cluster, you can run `cluster peer create` on the remote cluster to accept the relationship.

**Before you begin**
- You must have created intercluster LIFs on every node in the clusters being peered.
- The cluster administrators must have agreed on the passphrase each cluster will use to authenticate itself to the other.

**Steps**

1. On the data protection destination cluster, create a peer relationship with the data protection source cluster:
   
   ```
   cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace
   
   You can ignore the `-ipspace` option if you are not using a custom IPspace. For complete command syntax, see the man page.
   
   Example
   
   The following example creates a cluster peer relationship with the remote cluster at intercluster LIF IP addresses 192.168.2.201 and 192.168.2.202:
   
   ```bash
   cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   
   Enter the passphrase for the peer relationship when prompted.
   ```
   
   2. On the data protection source cluster, authenticate the source cluster to the destination cluster:

   ```
   cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace
   
   For complete command syntax, see the man page.
   
   Example
   
   The following example authenticates the local cluster to the remote cluster at intercluster LIF IP addresses 192.140.112.203 and 192.140.112.204:
   
   ```bash
   cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```
   
   Enter the passphrase for the peer relationship when prompted.
3. Verify that the cluster peer relationship was created:

   `cluster peer show -instance`

   For complete command syntax, see the man page.

   **Example**

   ```
   cluster01::> cluster peer show -instance
   Peer Cluster Name: cluster01
   Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
   Availability: Available
   Remote Cluster Name: cluster02
   Active IP Addresses: 192.168.2.201,192.168.2.202
   Cluster Serial Number: 1-80-000013
   ```

4. Check the connectivity and status of the nodes in the peer relationship:

   `cluster peer health show`

   For complete command syntax, see the man page.

   **Example**

   ```
   cluster01::> cluster peer health show
   Node       cluster-Name                Node-Name
   Ping-Status               RDB-Health  Cluster-Health  Avail...
   ---------- --------------------------- ---------  --------------- --------
   cluster01-01                  cluster02     cluster02-01
   Data: interface_reachable    ICMP: interface_reachable true  true  true
   cluster02-02
   Data: interface_reachable    ICMP: interface_reachable true  true  true
   cluster01-02                  cluster02     cluster02-01
   Data: interface_reachable    ICMP: interface_reachable true  true  true
   cluster02-02
   Data: interface_reachable    ICMP: interface_reachable true  true  true
   ```

**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.

**Related information**

*Logical storage management*

**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
```

### 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] 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

Implementing the MetroCluster configuration

You must run the metrocluster configure command to start data protection in a MetroCluster configuration.

Before you begin

- There should be at least two non-root mirrored data aggregates on each cluster. Additional data aggregates can be either mirrored or unmirrored.
  You can verify this with the storage aggregate show command.

  **Note:** If you want to use a single mirrored data aggregate, then see *step 1* on page 207 for instructions.

- The ha-config state of the controllers and chassis must be mcc.
About this task

You issue the `metrocluster configure` command once, on any of the nodes, to enable the MetroCluster configuration. You do not need to issue the command on each of the sites or nodes, and it does not matter which node or site you choose to issue the command on.

The `metrocluster configure` 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. Configure the MetroCluster in the following format:

<table>
<thead>
<tr>
<th>If your MetroCluster configuration has...</th>
<th>Then do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple data aggregates</td>
<td>From any node’s prompt, configure MetroCluster:</td>
</tr>
<tr>
<td></td>
<td><code>metrocluster configure node-name</code></td>
</tr>
<tr>
<td>A single mirrored data aggregate</td>
<td>a. From any node's prompt, change to the advanced privilege level:</td>
</tr>
<tr>
<td></td>
<td><code>set -privilege advanced</code></td>
</tr>
<tr>
<td></td>
<td>You need to respond with y when you are prompted to continue into advanced mode and you see the advanced mode prompt (*&gt;).</td>
</tr>
<tr>
<td></td>
<td>b. Configure the MetroCluster with the <code>-allow-with-one-aggregate true</code> parameter:</td>
</tr>
<tr>
<td></td>
<td><code>metrocluster configure -allow-with-one-aggregate true node-name</code></td>
</tr>
<tr>
<td></td>
<td>c. Return to the admin privilege level:</td>
</tr>
<tr>
<td></td>
<td><code>set -privilege admin</code></td>
</tr>
</tbody>
</table>

Example

*Note:* The best practice is to have multiple data aggregates. If the first DR group has only one aggregate and you want to add a DR group with one aggregate, you must move the metadata volume off the single data aggregate. For more information on this procedure, see *Moving a metadata volume in MetroCluster configurations.*

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

```
cluster_A::*> metrocluster configure -node-name controller_A_1
[Job 121] Job succeeded: Configure is successful.
```

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

<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>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_A_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.

a. Verify the configuration from site A:

```bash
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>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>Remote: cluster_B</td>
<td>Configuration state configured</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:

```bash
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>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>Remote: cluster_A</td>
<td>Configuration state configured</td>
<td></td>
</tr>
</tbody>
</table>
```

**Configuring in-order delivery or out-of-order delivery of frames on ONTAP software**

You must configure either in-order delivery (IOD) or out-of-order delivery (OOD) of frames according to the fibre channel (FC) switch configuration. If the FC switch is configured for IOD, then
the ONTAP software must be configured for IOD. Similarly, if the FC switch is configured for OOD, then ONTAP must be configured for OOD.

**Step**

1. Configure ONTAP to operate either IOD or OOD of frames.
   - By default, IOD of frames is enabled in ONTAP. To check the configuration details:
     a. Enter advanced mode:
        ```
        set advanced
        ```
     b. Verify the settings:
        ```
        metrocluster interconnect adapter show
        ```
        
        | Node Port Number | Adapter Name  | Type | Status | Enabled? | IP Address  | Port |
        |------------------|---------------|------|--------|---------|-------------|------|
        | mcc4-b1 17.0.1.2 | fcvi_device_0 | FC-VI| Up     | false   | 17.0.1.2    | 6a   |
        | mcc4-b1 18.0.0.2 | fcvi_device_1 | FC-VI| Up     | false   | 18.0.0.2    | 6b   |
        | mcc4-b1 192.0.5.193 | mlx4_0 | IB    | Down   | false   | 192.0.5.193 | ib2a |
        | mcc4-b1 192.0.5.194 | mlx4_0 | IB    | Up     | false   | 192.0.5.194 | ib2b |
        | mcc4-b2 17.0.2.2 | fcvi_device_0 | FC-VI| Up     | false   | 17.0.2.2    | 6a   |
        | mcc4-b2 18.0.1.2 | fcvi_device_1 | FC-VI| Up     | false   | 18.0.1.2    | 6b   |
        | mcc4-b2 192.0.2.9 | mlx4_0 | IB    | Down   | false   | 192.0.2.9   | ib2a |
        | mcc4-b2 192.0.2.10 | mlx4_0 | IB    | Up     | false   | 192.0.2.10  | ib2b |
        
        8 entries were displayed.

   - The following steps must be performed on each node to configure OOD of frames:
     a. Enter advanced mode:
        ```
        set advanced
        ```
     b. Verify the MetroCluster configuration settings:
        ```
        metrocluster interconnect adapter show
        ```
        
        | Node Port Number | Adapter Name  | Type | Status | Enabled? | IP Address  | Port |
        |------------------|---------------|------|--------|---------|-------------|------|
        | mcc4-b1 6a       | fcvi_device_0 | FC-VI| Up     | false   | 17.0.1.2    |       |
        | mcc4-b1 6b       | fcvi_device_1 | FC-VI| Up     | false   | 18.0.0.2    |       |
        | mcc4-b1 ib2a     | mlx4_0        | IB   | Down   | false   | 192.0.5.193 |       |
        | mcc4-b1 ib2b     | mlx4_0        | IB   | Up     | false   | 192.0.5.194 |       |
        | mcc4-b2 6a       | fcvi_device_0 | FC-VI| Up     | false   | 17.0.2.2    |       |
        | mcc4-b2 6b       | fcvi_device_1 | FC-VI| Up     | false   | 18.0.1.2    | 6b   |
        | mcc4-b2 ib2a     | mlx4_0        | IB   | Down   | false   | 192.0.2.9   |       |
        | mcc4-b2 ib2b     | mlx4_0        | IB   | Up     | false   | 192.0.2.10  |       |
        
        8 entries were displayed.
c. Enable OOD on node “mcc4-b1” and node “mcc4-b2”:

```
mcc4-b1:siteB::*> metrocluster interconnect adapter modify -node mcc4-b1 -is-ood-enabled true
mcc4-b2:siteB::*> metrocluster interconnect adapter modify -node mcc4-b2 -is-ood-enabled true
```  

```
mcc4-b1      fcvi_device_0   FC-VI   Up     true      17.0.1.2        6a
mcc4-b1      fcvi_device_1   FC-VI   Up     true      18.0.0.2        6b
mcc4-b1      mlx4_0          IB      Down   false     192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB      Up     false     192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI   Up     true      17.0.2.2        6a
mcc4-b2      fcvi_device_1   FC-VI   Up     true      18.0.1.2        6b
mcc4-b2      mlx4_0          IB      Down   false     192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB      Up     false     192.0.2.10
ib2b
8 entries were displayed.
```  

d. Verify the settings:

```
mcc4-b1:siteB::*> metrocluster interconnect adapter show
mcc4-b1:siteB::*> metrocluster interconnect adapter show
```

```
<table>
<thead>
<tr>
<th>Node Number</th>
<th>Adapter Name</th>
<th>Type</th>
<th>Status</th>
<th>Enabled?</th>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcc4-b1</td>
<td>fcvi_device_0</td>
<td>FC-VI</td>
<td>Up</td>
<td>true</td>
<td>17.0.1.2</td>
<td>6a</td>
</tr>
<tr>
<td>mcc4-b1</td>
<td>fcvi_device_1</td>
<td>FC-VI</td>
<td>Up</td>
<td>true</td>
<td>18.0.0.2</td>
<td>6b</td>
</tr>
<tr>
<td>mcc4-b1</td>
<td>mlx4_0</td>
<td>IB</td>
<td>Down</td>
<td>false</td>
<td>192.0.5.193</td>
<td></td>
</tr>
<tr>
<td>ib2a</td>
<td>mlx4_0</td>
<td>IB</td>
<td>Up</td>
<td>false</td>
<td>192.0.5.194</td>
<td></td>
</tr>
<tr>
<td>mcc4-b2</td>
<td>fcvi_device_0</td>
<td>FC-VI</td>
<td>Up</td>
<td>true</td>
<td>17.0.2.2</td>
<td>6a</td>
</tr>
<tr>
<td>mcc4-b2</td>
<td>fcvi_device_1</td>
<td>FC-VI</td>
<td>Up</td>
<td>true</td>
<td>18.0.1.2</td>
<td>6b</td>
</tr>
<tr>
<td>mcc4-b2</td>
<td>mlx4_0</td>
<td>IB</td>
<td>Down</td>
<td>false</td>
<td>192.0.2.9</td>
<td></td>
</tr>
<tr>
<td>ib2a</td>
<td>mlx4_0</td>
<td>IB</td>
<td>Up</td>
<td>false</td>
<td>192.0.2.10</td>
<td></td>
</tr>
<tr>
<td>ib2b</td>
<td>mlx4_0</td>
<td>IB</td>
<td>Up</td>
<td>false</td>
<td>192.0.2.10</td>
<td></td>
</tr>
</tbody>
</table>

8 entries were displayed.
```

Configuring SNMPv3 in a MetroCluster configuration

**Before you begin**

The authentication and privacy protocols on the switches and on the ONTAP system must be the same.

**About this task**

ONTAP currently supports AES-128 and AES-256 encryption.

**Steps**

1. Create an SNMP user for each switch from the controller prompt:

```
security login create
```

**Example**

```
Controller_A_1::> security login create -user-or-group-name monitoringv3ro -application snmp -authentication-method usm -role none -remote-switch-ipaddress 10.10.10.10
```

2. Respond to the following prompts as required at your site:

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256) [none]: sha
```
Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]: aes128
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:

**Note:** The same username can be added to different switches with different IP addresses.

3. Create an SNMP user for the rest of the switches.

The following example shows how to create a username for a switch with the IP address 10.10.10.

```
Controller_A_1:/> security login create -user-or-group-name monitoringv3ro -application snmp -authentication-method usm -role none -remote-switch-ipaddress 10.10.10
```

4. Check that there is one login entry for each switch:

```
security login show
```

**Example**

```
Controller_A_1:/> security login show -user-or-group-name monitoringv3ro -fields remote-switch-ipaddress

<table>
<thead>
<tr>
<th>vserver</th>
<th>user-or-group-name</th>
<th>application</th>
<th>authentication-method</th>
<th>remote-switch-ipaddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch_1_A:&gt;</td>
<td>monitoringv3ro</td>
<td>snmp</td>
<td>usm</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>switch_1_A:&gt;</td>
<td>monitoringv3ro</td>
<td>snmp</td>
<td>usm</td>
<td>10.10.10.11</td>
</tr>
<tr>
<td>switch_1_A:&gt;</td>
<td>mmonitoringv3ro</td>
<td>snmp</td>
<td>usm</td>
<td>10.10.10.12</td>
</tr>
<tr>
<td>switch_1_A:&gt;</td>
<td>monitoringv3ro</td>
<td>snmp</td>
<td>usm</td>
<td>10.10.10.13</td>
</tr>
</tbody>
</table>

4 entries were displayed.
```

5. Configure SNMPv3 on the switches from the switch prompt:

```
snmpconfig --set snmpv3
```

**Example**

```
SiteA:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user database will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00] [2]
```

The example shows how to configure a read-only user. You can adjust the RW users if needed. You should also set passwords on unused accounts to secure them.
Configuring MetroCluster components for health monitoring

You must perform some special configuration steps before monitoring the components in a MetroCluster configuration.

About this task

These tasks apply only to systems with FC-to-SAS bridges.

Note:

• You should place bridges and a node management LIF in a dedicated network to avoid interference from other sources.

• If you use a dedicated network for Health Monitoring, then each node must have a node management LIF in that dedicated network.

Steps

1. Configuring the MetroCluster FC switches for health monitoring on page 212
2. Configuring FC-to-SAS bridges for health monitoring on page 213

Configuring the MetroCluster FC switches for health monitoring

In a fabric-attached MetroCluster configuration, you must perform some additional configuration steps to monitor the FC switches.

Steps

1. Add a switch with an IP address to each MetroCluster node:

   `storage switch add -address ipaddress`

   This command must be repeated on all four switches in the MetroCluster configuration.

   Note: Brocade 7840 FC switches and all alerts are supported in health monitoring, except NoISLPresent_Alert

Example

The following example shows the command to add a switch with IP address 10.10.10.10:

   `controller_A_1::> storage switch add -address 10.10.10.10`

2. Verify that all switches are properly configured:

   `storage switch show`

   It might take up to 15 minutes to reflect all data due to the 15-minute polling interval.

Example

The following example shows the command given to verify that the MetroCluster FC switches are configured:

```
controller_A_1::> storage switch show
<table>
<thead>
<tr>
<th>Fabric</th>
<th>Switch Name</th>
<th>Vendor</th>
<th>Model</th>
<th>Switch WWN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000000533a9e7a6</td>
<td>brcd6505-fcs40</td>
<td>Brocade</td>
<td>Brocade6505</td>
<td>1000000533a9e7a6</td>
<td>OK</td>
</tr>
<tr>
<td>1000000533a9e7a6</td>
<td>brcd6505-fcs42</td>
<td>Brocade</td>
<td>Brocade6505</td>
<td>1000000533d3660a</td>
<td>OK</td>
</tr>
<tr>
<td>1000000533ed94d1</td>
<td>brcd6510-fcs44</td>
<td>Brocade</td>
<td>Brocade6510</td>
<td>1000000533eda031</td>
<td>OK</td>
</tr>
</tbody>
</table>
```
If the worldwide name (WWN) of the switch is shown, the ONTAP health monitor can contact and monitor the FC switch.

Related information

System administration

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>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

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
------------------  ------------- ------------  --------------  ------
Model              Bridge WWN
------------------    ----------
ATTO_10.10.20.10    att001        true          ok              Atto   FibreBridge
7500N  20000010867038c0
ATTO_10.10.20.11    att002        true          ok              Atto   FibreBridge
7500N  20000010867033c0
ATTO_10.10.20.12    att003        true          ok              Atto   FibreBridge
7500N  20000010867030c0
ATTO_10.10.20.13    att004        true          ok              Atto   FibreBridge
7500N  2000001086703b80

4 entries were displayed
```

controller_A_1::>
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.
```

Related information

* Disk and aggregate management
* Network and LIF management
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.

Verifying local HA operation

If you have a four-node MetroCluster configuration, you should verify the operation of the local HA pairs in the MetroCluster configuration. This is not required for two-node configurations.

**About this task**

Two-node MetroCluster configurations do not consist of local HA pairs and this task does not apply. The examples in this task use standard naming conventions:

- cluster_A
  - controller_A_1
  - controller_A_2
- cluster_B
  - controller_B_1
  - controller_B_2

**Steps**

1. On cluster_A, perform a failover and giveback in both directions.

   a. Confirm that storage failover is enabled:

      ```
      storage failover show
      ```

   **Example**

      The output should indicate that takeover is possible for both nodes:
b. Take over controller_A_2 from controller_A_1:

```
storage failover takeover controller_A_2
```

You can use the `storage failover show-takeover` command to monitor the progress of the takeover operation.

c. Confirm that the takeover is complete:

```
storage failover show
```

**Example**

The output should indicate that controller_A_1 is in takeover state, meaning that it has taken over its HA partner:

```
cluster_A::> storage failover show

Takeover
Node         Partner        Possible State Description
-------------- -------------- -------- ---------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2
controller_A_2 controller_A_1 true     Connected to controller_A_1

2 entries were displayed.
```

d. Give back controller_A_2:

```
storage failover giveback controller_A_2
```

You can use the `storage failover show-giveback` command to monitor the progress of the giveback operation.

e. Confirm that storage failover has returned to a normal state:

```
storage failover show
```

**Example**

The output should indicate that takeover is possible for both nodes:

```
cluster_A::> storage failover show

Takeover
Node         Partner        Possible State Description
-------------- -------------- -------- ---------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2
controller_A_2 controller_A_1 true     Connected to controller_A_1

2 entries were displayed.
```

f. Repeat the previous substeps, this time taking over controller_A_1 from controller_A_2.

2. Repeat the preceding steps on cluster_B.
Related information

High-availability configuration

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

Installing the MetroCluster Tiebreaker software

You can download and install Tiebreaker software to monitor the two clusters and the connectivity status between them from a third site. Doing so enables each partner in a cluster to distinguish between an ISL failure (when inter-site links are down) and a site failure.

Before you begin

You must have a Linux host available that has network connectivity to both clusters in the MetroCluster configuration.

Steps

1. Go to MetroCluster Tiebreaker Software Download page.

   NetApp Downloads: MetroCluster Tiebreaker for Linux

2. Follow the directions to download the Tiebreaker software and documentation.

Protecting configuration backup files

You can provide additional protection for the cluster configuration backup files by specifying a remote URL (either HTTP or FTP) where the configuration backup files will be uploaded in addition to the default locations in the local cluster.

Step

1. Set the URL of the remote destination for the configuration backup files:

   system configuration backup settings modify URL-of-destination

   The System Administration Guide contains additional information under the section Managing configuration backups.

   System administration

Related information

System administration
Testing the MetroCluster configuration

You can test failure scenarios to confirm the correct operation of the MetroCluster configuration.

Verifying negotiated switchover

You can test the negotiated (planned) switchover operation to confirm uninterrupted data availability.

About this task

This test validates that data availability is not affected (except for Microsoft Server Message Block (SMB) and Solaris Fibre Channel protocols) by switching the cluster over to the second data center.

This test should take about 30 minutes.

This procedure has the following expected results:

• The `metrocluster switchover` command will present a warning prompt.
  If you respond `yes` to the prompt, the site from where the command is issued should switch over to the partner site.

• Nodes at the partner site should shut down gracefully and remain at the LOADER> prompt.

Steps

1. Confirm that all nodes are in the configured state and normal mode:

   `metrocluster node show`

   Example

   ```
   cluster_A::> metrocluster node show
   Clusters: 1
   Configuration State: configured
   Mode: normal
   Local: cluster_A
   Remote: cluster_B
   ```

2. Begin the switchover operation:

   `metrocluster switchover`

   Example

   ```
   cluster_A::> metrocluster switchover
   Warning: negotiated switchover is about to start. It will stop all the data Vservers on cluster "cluster_B" and automatically re-start them on cluster "cluster_A". It will finally gracefully shutdown cluster "cluster_B".
   ```

3. Confirm that the local cluster is in the configured state and switchover mode:

   `metrocluster node show`

   Example

   ```
   cluster_A::> metrocluster node show
   Clusters: 1
   Configuration State: configured
   Mode: normal
   Local: cluster_A
   Remote: cluster_B
   ```
4. Confirm that the switchover operation was successful:

   `metrocluster operation show`

   **Example**

   ```bash
   cluster_A::> metrocluster operation show
   Operation: switchover
   State: successful
   Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
   Errors: -
   ```

5. Use the `vserver show` and `network interface show` commands to verify that DR SVMs and LIFs have come online.

---

**Verifying healing and manual switchback**

You can test the healing and manual switchback operations to verify that data availability is not affected (except for SMB and Solaris FC configurations) by switching back the cluster to the original data center after a negotiated switchover.

**About this task**

This test should take about 30 minutes.

The expected result of this procedure is that services should be switched back to their home nodes.

The healing steps are not required on systems running ONTAP 9.5 or later, on which healing is performed automatically after a negotiated switchover. On systems running ONTAP 9.6 and later, healing is also performed automatically after unscheduled switchover.

**Steps**

1. If the system is running ONTAP 9.4 or earlier, heal the data aggregate:

   `metrocluster heal aggregates`

   **Example**

   The following example shows the successful completion of the command:

   ```bash
   cluster_A::> metrocluster heal aggregates
   [Job 936] Job succeeded: Heal Aggregates is successful.
   ```

2. If it is required by your configuration, heal the root aggregate:

   `metrocluster heal root-aggregates`

   This step is required on the following configurations:

   - MetroCluster FC configurations.
   - MetroCluster IP configurations running ONTAP 9.4 or earlier.

   **Example**

   The following example shows the successful completion of the command:
3. Verify that healing is completed:

    `metrocluster node show`

**Example**

The following example shows the successful completion of the command:

```
cluster_A::> metrocluster node show
DR                       Configuration     DR
Group Cluster Node        State          Mirroring Mode
------------------------- -------------------------
1  cluster_A               configured     enabled heal roots completed
    node_A_1                configured     enabled heal roots completed
    cluster_B               unreachable    - switched over
    node_B_2                unreachable    - switched over
42 entries were displayed.
```

If the automatic healing operation fails for any reason, you must issue the `metrocluster heal` commands manually as done in ONTAP versions prior to ONTAP 9.5. You can use the `metrocluster operation show` and `metrocluster operation history show` commands to monitor the status of healing and determine the cause of a failure.

4. Verify that all aggregates are mirrored:

    `storage aggregate show`

**Example**

The following example shows that all aggregates have a RAID Status of `mirrored`:

```
cluster_A::> storage aggregate show
Cluster Aggregates:
Aggregation Size     Available Used% State   #Vols  Nodes       RAID Status
------------------------------- --------- ----- ------- ------- --------------
data_cluster 4.19TB    4.13TB    2% online       8 node_A_1    raid_dp, mirrored, normal
root_cluster 715.5GB   212.7GB   70% online       1 node_A_1    raid4, mirrored, normal

Cluster B Switched Over Aggregates:
Aggregation Size     Available Used% State   #Vols  Nodes       RAID Status
------------------------------- --------- ----- ------- ------- --------------
data_cluster_B 4.19TB    4.11TB    2% online       5 node_A_1    raid_dp, mirrored, normal
root_cluster_B -        -         - unknown      - node_A_1   -
```

5. Boot nodes from the disaster site.

6. Check the status of switchback recovery:

    `metrocluster node show`

**Example**

```
cluster_A::> metrocluster node show
DR                       Configuration  DR
Group Cluster Node        State          Mirroring Mode
------------------------- -------------------------
1  cluster_A              configured     enabled heal roots completed
    node_A_1                configured     enabled heal roots completed
```

```
Testing the MetroCluster configuration | 221```
7. Perform the switchback:

```snippet
metrocluster switchback
```

Example

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful. Verify switchback
```

8. Confirm status of the nodes:

```snippet
metrocluster node show
```

Example

```
cluster_A::> metrocluster node show
DR Group Cluster Node Configuration DR
          --------------- -------------- ---------
--------- ------------- -------------- ---------
1       cluster_A     node_A_1   configured enabled normal
        cluster_B     node_B_2   configured enabled normal

2 entries were displayed.
```

9. Confirm status of the metrocluster operation:

```snippet
metrocluster operation show
```

Example

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: 2/6/2016 13:54:25
End Time: 2/6/2016 13:56:15
Errors: -
```

---

**Loss of a single FC-to-SAS bridge**

You can test the failure of a single FC-to-SAS bridge to make sure there is no single point of failure.

**About this task**

This test should take about 15 minutes.

This procedure has the following expected results:

- Errors should be generated as the bridge is switched off.
- No failover or loss of service should occur.
• Only one path from the controller module to the drives behind the bridge is available.

Steps
1. Turn off the power supplies of the bridge.
2. Confirm that the bridge monitoring indicates an error:
   
   storage bridge show

   Example

   ```
   clustera::> storage bridge show
   Bridge  Symbolic Name Vendor  Model     Bridge WWN       Is Monitored Status
   ------ ------------- ------- --------- ----------------- --------- -------
   ATTO_10.65.57.145  bridge_A_1    Atto    FibreBridge 6500N
   200000108662d46c true      error
   ```

3. Confirm that drives behind the bridge are available with a single path:
   
   storage disk error show

   Example

   ```
   clustera::> storage disk error show
   Disk             Error Type        Error Text
   ----------- ----------------- --------------------------------------------
   1.0.0            onedomain         1.0.0 (5000cca057729118): All paths to this array LUN
   are connected to the same fault domain. This is a single point of failure.
   1.0.1            onedomain         1.0.1 (5000cca057727364): All paths to this array LUN
   are connected to the same fault domain. This is a single point of failure.
   1.0.2            onedomain         1.0.2 (5000cca05772e9d4): All paths to this array LUN
   are connected to the same fault domain. This is a single point of failure.
   ...
   1.0.23           onedomain         1.0.23 (5000cca05772e9d4): All paths to this array LUN
   are connected to the same fault domain. This is a single point of failure.
   ```

Verifying operation after power line disruption

You can test the MetroCluster configuration's response to the failure of a PDU.

About this task

The best practice is for each power supply unit (PSU) in a component to be connected to separate power supplies. If both PSUs are connected to the same power distribution unit (PDU) and an electrical disruption occurs, the site could down or a complete shelf might become unavailable. Failure of one power line is tested to confirm that there is no cabling mismatch that could cause a service disruption.

This test should take about 15 minutes.

This test requires turning off power to all left-hand PDUs and then all right-hand PDUs on all of the racks containing the MetroCluster components.

This procedure has the following expected results:

• Errors should be generated as the bridge is switched off.
• No failover or loss of service should occur.
• Only one path from the controller module to the drives behind the bridge is available.
Steps

1. Turn off the power of the PDUs on the left-hand side of the rack containing the MetroCluster components.

2. Monitor the result on the console by using the `system environment sensors show -state fault` and `storage shelf show -errors` commands.

Example

```
cluster_A::> system environment sensors show -state fault

----------------- -------------------- ---------- ---------- ----------
              ---------------------- ------- --------- --------- ------- -------
node_A_1
    PSU1     fault       PSU_OFF
    PSU1 Pwr In OK fault    FAULT
node_A_2
    PSU1     fault       PSU_OFF
    PSU1 Pwr In OK fault    FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors

Shelf Name: 1.1
    Shelf UID: 50:0a:09:80:03:6c:44:d5
    Serial Number: SHFHU1443000059

Error Type Description
---------------------- ------------------------------------------
Power                  Critical condition is detected in storage shelf
                        power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Turn the power back on to the left-hand PDUs.

4. Make sure that ONTAP clears the error condition.

5. Repeat the previous steps with the right-hand PDUs.

Verifying operation after a switch fabric failure

You can disable a switch fabric to show that data availability is not affected by the loss.

About this task

This test should take about 15 minutes.

The expected result of this procedure is that disabling a fabric results in all cluster interconnect and disk traffic flowing to the other fabric.

In the examples shown, switch fabric 1 is disabled. This fabric consists of two switches, one at each MetroCluster site:

- FC_switch_A_1 on cluster_A
- FC_switch_B_1 on cluster_B
Steps

1. Disable connectivity to one of the two switch fabrics in the MetroCluster configuration:
   a. Disable the first switch in the fabric:
      ```
      switchdisable
      ```
      Example
      ```
      FC_switch_A_1::> switchdisable
      ```
   b. Disable the second switch in the fabric:
      ```
      switchdisable
      ```
      Example
      ```
      FC_switch_B_1::> switchdisable
      ```

2. Monitor the result on the console of the controller modules.
   You can use the following commands to check the cluster nodes to make sure that all data is still being served. The command output shows missing paths to disks. This is expected.
   - vserver show
   - network interface show
   - aggr show
   - system node run nodename -command storage show disk -p
   - storage disk error show

3. Reenable connectivity to one of the two switch fabrics in the MetroCluster configuration:
   a. Reenable the first switch in the fabric:
      ```
      switchenable
      ```
      Example
      ```
      FC_switch_A_1::> switchenable
      ```
   b. Reenable the second switch in the fabric:
      ```
      switchenable
      ```
      Example
      ```
      FC_switch_B_1::> switchenable
      ```

4. Wait at least 10 minutes and then repeat the above steps on the other switch fabric.
Verifying operation after loss of a single storage shelf

You can test the failure of a single storage shelf to verify that there is no single point of failure.

**About this task**

This procedure has the following expected results:

- An error message should be reported by the monitoring software.
- No failover or loss of service should occur.
- Mirror resynchronization starts automatically after the hardware failure is restored.

**Steps**

1. Check the storage failover status:
   
   ```
   storage failover show
   ```

   **Example**
   
   ```
   cluster_A::> storage failover show
   Node           Partner        Possible State Description
   --------------- -------------- --------
   ________________________________
   node_A_1       node_A_2       true     Connected to node_A_2
   node_A_2       node_A_1       true     Connected to node_A_1
   2 entries were displayed.
   ```

2. Check the aggregate status:
   
   ```
   storage aggregate show
   ```

   **Example**
   
   ```
   cluster_A::> storage aggregate show
   cluster Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
   --------- -------- --------- ----- ------- ------ ---------------- ------------
   node_A_1data01_mirrored 4.15TB    3.40TB   18% online       3 node_A_1       raid_dp, mirrored, normal
   node_A_1root  707.7GB   34.29GB   95% online       1 node_A_1       raid_dp, mirrored, normal
   node_A_2_data01_mirrored 4.15TB    4.12TB   1% online       2 node_A_2       raid_dp, mirrored, normal
   node_A_2_data02_unmirrored 2.18TB    2.18TB   0% online       1 node_A_2       raid_dp, normal
   node_A_2_root  707.7GB   34.27GB   95% online       1 node_A_2       raid_dp, mirrored, normal
   ```

3. Verify that all data SVMs and data volumes are online and serving data:
   
   ```
   vserver show -type data
   network interface show -fields is-home false
   volume show !vol0,!MDV*
   ```
Example

```bash
cluster_A::> vserver show -type data
Vserver    Type    Subtype    State      State       Volume     Aggregate
----------- ------- ---------- ---------- ----------- ---------- ----------
SVM1        data    sync-source           running     SVM1_root  node_A_1_data01_mirrored
SVM2        data    sync-source              running     SVM2_root
```

```bash
cluster_A::> network interface show -fields is-home false
There are no entries matching your query.
```

```bash
cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
SVM1      SVM1_root   node_A_1data01_mirrored online     RW         10GB     9.50GB    5%
SVM1      SVM1_data_vol node_A_1data01_mirrored online     RW         10GB     9.49GB    5%
SVM2      SVM2_root   node_A_2_data01_mirrored online     RW         10GB     9.49GB    5%
SVM2      SVM2_data_vol node_A_2_data02_unmirrored online     RW          1GB   972.6MB    5%
```

4. Identify a shelf in Pool 1 for node node_A_2 to power off to simulate a sudden hardware failure:

```
storage aggregate show -r -node node_name !*root
```

The shelf you select must contain drives that are part of a mirrored data aggregate.

Example

In the following example, shelf ID 31 is selected to fail.

```bash
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
  RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block checksums)
  Usable Physical
  Position Disk Pool Type RPM  Size  Size Status
  -------- ------------------------------------------
  dparity  2.30.3   0  BSAS  7200  827.7GB  828.0GB (normal)
  parity   2.30.4   0  BSAS  7200  827.7GB  828.0GB (normal)
  data 2.30.6    0  BSAS  7200  827.7GB  828.0GB (normal)
  data 2.30.8    0  BSAS  7200  827.7GB  828.0GB (normal)
  data 2.30.5    0  BSAS  7200  827.7GB  828.0GB (normal)
```

15 entries were displayed.
5. Physically power off the shelf that you selected.

6. Check the aggregate status again:

```
storage aggregate show
storage aggregate show -r -node node_A_2 !*root
```

**Example**

The aggregate with drives on the powered-off shelf should have a degraded RAID status, and drives on the affected plex should have a failed status, as shown in the following example:

```
cluster_A::> storage aggregate show

Aggregate    Size     Available Used%  State    #Vols  Nodes          RAID Status
--------- -------- --------- ----- ------- ------ ---------------- ------------
node_A_1data01_mirrored 4.15TB    3.40TB    18%  online    3 node_A_1       raid_dp, mirrored, normal
node_A_1root     707.7GB   34.29GB    95%  online    1 node_A_1       raid_dp, mirrored, normal
node_A_2_data01_mirrored 4.15TB    4.12TB    1%   online    2 node_A_2       raid_dp, mirror degraded
node_A_2_data02_unmirrored 2.18TB   2.18TB    0%   online    1 node_A_2       raid_dp, normal
node_A_2_root     707.7GB   34.27GB    95%  online    1 node_A_2       raid_dp, mirror degraded

cluster_A::> storage aggregate show -r -node node_A_2 !*root

Owner Node: node_A_2
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded) (block checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block checksums)
Usable Physical
Position Disk          Pool Type  RPM     Size     Size Status
-------- ---------------------- ---- ----- ------ -------- --------
dparity  2.30.3                      0   BSAS    7200  827.7GB  828.0GB (normal)
parity  2.30.4                      0   BSAS    7200  827.7GB  828.0GB (normal)
data    2.30.6                      0   BSAS    7200  827.7GB  828.0GB (normal)
data    2.30.8                      0   BSAS    7200  827.7GB  828.0GB (normal)
data    2.30.5                      0   BSAS    7200  827.7GB  828.0GB (normal)

Plex: /node_A_2_data02_unmirrored/plex4 (offline, failed, inactive, pool1)
   RAID Group /node_A_2_data02_unmirrored/plex4/rg0 (partial, none checksums)
Usable Physical
Position Disk          Pool Type  RPM     Size     Size Status
-------- ---------------------- ---- ----- ------ -------- --------
dparity FAILED         -       -       -       -       - (failed)
parity FAILED         -       -       -       -       - (failed)
data FAILED            -       -       -       -       - (failed)
data FAILED            -       -       -       -       - (failed)
data FAILED            -       -       -       -       - (failed)

Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block checksums)
Plex: /node_A_2_data02_unmirrored/plex5 (online, normal, active, pool0)
   RAID Group /node_A_2_data02_unmirrored/plex5/rg0 (normal, block checksums)
Usable Physical
Position Disk          Pool Type  RPM     Size     Size Status
-------- ---------------------- ---- ----- ------ -------- --------
dparity  2.30.12                     0   BSAS    7200  827.7GB  828.0GB (normal)
parity  2.30.22                     0   BSAS    7200  827.7GB  828.0GB (normal)
data    2.30.21                     0   BSAS    7200  827.7GB  828.0GB (normal)
data    2.30.20                     0   BSAS    7200  827.7GB  828.0GB (normal)
data    2.30.14                     0   BSAS    7200  827.7GB  828.0GB (normal)
15 entries were displayed.
```

7. Verify that the data is being served and that all volumes are still online:

```
vserver show -type data
network interface show -fields is-home false
volume show !vol0,!MDV*
```
Example

```
cluster_A::> vserver show -type data
cluster_A::> vserver show -type data
Vserver             Type       Subtype   Admin   Operational Root
----------- ------- --------- ------- ---------------- 
SVM1        data    sync-source running   SVM1_root  node_A_1_data01_mirrored
SVM2        data    sync-source running   SVM2_root  node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.
```

```
cluster_A::> volume show !vol0,!MDV*
Vserver       Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
SVM1         SVM1_root    node_A_1data01_mirrored online     RW         10GB     9.50GB    5%
SVM1         SVM1_data_vol node_A_1data01_mirrored online     RW         10GB     9.49GB    5%
SVM2         SVM2_root    node_A_1data01_mirrored online     RW         10GB     9.49GB    5%
SVM2         SVM2_data_vol node_A_2_data02_unmirrored online     RW         1GB    972.6MB    5%
```

8. Physically power on the shelf.  
   Resynchronization starts automatically.

9. Verify that resynchronization has started:  
   `storage aggregate show`

Example

The affected aggregate should have a resyncing RAID status, as shown in the following example:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate       Size Available Used% State   #Vols  Nodes            RAID Status
--------- -------- --------- ----- ------- ------ ---------------- ------------ 
node_A_1_data01_mirrored 4.15TB  3.40TB    18% online       3 node_A_1       raid_dp, mirrored, normal
node_A_1_root 707.7GB  34.29GB   95% online       1 node_A_1       raid_dp, mirrored, normal
node_A_2_data01_mirrored 4.15TB  4.12TB    1% online       2 node_A_2       raid_dp, resyncing
node_A_2_data02_unmirrored 2.18TB  2.18TB    0% online       1 node_A_2       raid_dp, normal
node_A_2_root 707.7GB  34.27GB   95% online       1 node_A_2       raid_dp, resyncing
```

10. Monitor the aggregate to confirm that resynchronization is complete:  
    `storage aggregate show`

Example

The affected aggregate should have a normal RAID status, as shown in the following example:
<table>
<thead>
<tr>
<th>Aggregate</th>
<th>Size</th>
<th>Available</th>
<th>Used%</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1data01_mirrored</td>
<td>4.15TB</td>
<td>3.40TB</td>
<td>18%</td>
<td>online</td>
<td>3</td>
<td>node_A_1</td>
<td>raid_dp, mirrored, normal</td>
</tr>
<tr>
<td>node_A_1root</td>
<td>707.7GB</td>
<td>34.29GB</td>
<td>95%</td>
<td>online</td>
<td>1</td>
<td>node_A_1</td>
<td>raid_dp, mirrored, normal</td>
</tr>
<tr>
<td>node_A_2_data01_mirrored</td>
<td>4.15TB</td>
<td>4.12TB</td>
<td>1%</td>
<td>online</td>
<td>2</td>
<td>node_A_2</td>
<td>raid_dp, normal</td>
</tr>
<tr>
<td>node_A_2_data02_unmirrored</td>
<td>2.18TB</td>
<td>2.18TB</td>
<td>0%</td>
<td>online</td>
<td>1</td>
<td>node_A_2</td>
<td>raid_dp, normal</td>
</tr>
<tr>
<td>node_A_2_root</td>
<td>707.7GB</td>
<td>34.27GB</td>
<td>95%</td>
<td>online</td>
<td>1</td>
<td>node_A_2</td>
<td>raid_dp, resyncing</td>
</tr>
</tbody>
</table>
Considerations when removing MetroCluster configurations

You can remove the MetroCluster configuration from all nodes in the MetroCluster configuration or all of the nodes in a disaster recovery (DR) group. After removing the MetroCluster configuration, all disk connectivity and interconnects should be adjusted to be in a supported state. If you need to remove the MetroCluster configuration, contact technical support.

Attention: You cannot reverse the MetroCluster unconfiguration. This process should only be done with the assistance of technical support.
Planning and installing a MetroCluster configuration with array LUNs

If you are using array LUNs in your MetroCluster configuration, you must plan the installation and follow the specific procedures for such a configuration. You can set up a MetroCluster configuration with either a mix of array LUNs and native disk shelves or only array LUNs.

Planning for a MetroCluster configuration with array LUNs

Creating a detailed plan for your MetroCluster configuration helps you understand the unique requirements for a MetroCluster configuration that uses LUNs on storage arrays. Installing a MetroCluster configuration involves connecting and configuring a number of devices, which might be done by different people. Therefore, the plan also helps you communicate with other people involved in the installation.

Supported MetroCluster configuration with array LUNs

You can set up either a MetroCluster configuration with array LUNs. Both stretch and fabric-attached configurations are supported. AFF systems are not supported with array LUNs.

The features supported on the MetroCluster configurations vary with the configuration types. The following table lists the features supported on the different types of MetroCluster configurations with array LUNs:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Fabric-attached configurations</th>
<th>Stretch configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Eight-node</td>
<td>Four-node</td>
</tr>
<tr>
<td>Number of controllers</td>
<td>Eight</td>
<td>Four</td>
</tr>
<tr>
<td>Uses an FC switch storage fabric</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses FC-to-SAS bridges</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports local HA</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Supports automatic switchover</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Related concepts

*Differences between the ONTAP MetroCluster configurations* on page 9
Requirements for a MetroCluster configuration with array LUNs

The ONTAP systems, storage arrays, and FC switches used in MetroCluster configurations must meet the requirements for such types of configurations. In addition, you must also consider the SyncMirror requirements for MetroCluster configurations with array LUNs.

Requirements for ONTAP systems

- The ONTAP systems must be identified as supported for MetroCluster configurations.
  
  **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.

  **Note:** You must refer to the alert details associated with any configuration that you select in the Interoperability Matrix.

- All the ONTAP systems in a MetroCluster configuration must be of the same model.

- FC-VI adapters must be installed in the appropriate slots for each ONTAP system, depending on the model.
  
  **NetApp Hardware Universe**

Requirements for storage arrays

- The storage arrays must be identified as supported for MetroCluster configurations.
  
  **NetApp Interoperability Matrix Tool**

- The storage arrays in the MetroCluster configuration must be symmetric:
  - The two storage arrays must be from the same supported vendor family and have the same firmware version installed.
    
    **FlexArray virtualization implementation for NetApp E-Series storage**
    **FlexArray virtualization implementation for third-party storage**
  - Disk types (for example, SATA, SSD, or SAS) used for mirrored storage must be the same on both storage arrays.
  - The parameters for configuring storage arrays, such as RAID type and tiering, must be the same across both sites.

Requirements for FC switches

- The switches and switch firmware must be identified as supported for MetroCluster configurations.
  
  **NetApp Interoperability Matrix Tool**

- Each fabric must have two FC switches.

- Each ONTAP system must be connected to storage using redundant components so that there is redundancy in case of device and path failures.

- FAS9000 storage systems support up to eight ISLs per fabric. Other storage system models support up to four ISLs per fabric.

  The switches must use the MetroCluster basic switch configuration, ISL settings, and FC-VI configurations.
SyncMirror requirements

- SyncMirror is required for a MetroCluster configuration.
- Two separate storage arrays, one at each site, are required for the mirrored storage.
- Two sets of array LUNs are required.
  One set is required for the aggregate on the local storage array (pool0) and another set is required at the remote storage array for the mirror of the aggregate (the other plex of the aggregate, pool1). The array LUNs must be of the same size for mirroring the aggregate.
- Unmirrored aggregates are also supported in the MetroCluster configuration. They are not protected in the event of a site disaster.

Installing and cabling the MetroCluster components in a configuration with array LUNs

For setting up a MetroCluster configuration with array LUNs, you must cable the storage controllers to the FC switches and cable the ISLs to link the sites. In addition, you must cable the storage arrays to the FC switches.

Steps

1. Racking the hardware components in a MetroCluster configuration with array LUNs on page 234
2. Preparing a storage array for use with ONTAP systems on page 235
3. Switch ports required for a MetroCluster configuration with array LUNs on page 235
4. Cabling the FC-VI and HBA ports in a MetroCluster configuration with array LUNs on page 243
5. Cabling the ISLs in a MetroCluster configuration with array LUNs on page 249
6. Cabling the cluster interconnect in eight- or four-node configurations on page 251
7. Cabling the cluster peering connections on page 251
8. Cabling the HA interconnect, if necessary on page 252
9. Cabling the management and data connections on page 252
10. Cabling storage arrays to FC switches in a MetroCluster configuration on page 252

Racking the hardware components in a MetroCluster configuration with array LUNs

You must ensure that the hardware components required to set up a MetroCluster configuration with array LUNs are properly racked.

About this task

You must perform this task at both the MetroCluster sites.

Steps

1. Plan the positioning of the MetroCluster components.
   The rack space depends on the platform model of the storage controllers, the switch types, and the number of disk shelf stacks in your configuration.
2. Properly ground yourself.
3. Install the storage controllers in the rack or cabinet.
Note: AFF systems are not supported with array LUNs.

**AFF A700 and FAS9000 Installation and Setup Instructions**

**FAS8200 Systems Installation and Setup Instructions**

**Installation and Setup Instructions FAS8040/FAS8060 Systems**

**Installation and setup Instructions FAS80xx Systems with I/O Expansion Modules**

**Installation and Setup Instructions FAS8020 systems**

**Installation and Setup Instructions 62xx Systems**

**Installation and Setup Instructions 32xx Systems**

4. Install the FC switches in the rack or cabinet.

### Preparing a storage array for use with ONTAP systems

Before you can begin setting up ONTAP systems in a MetroCluster configuration with array LUNs, the storage array administrator must prepare the storage for use with ONTAP.

#### Before you begin

The storage arrays, firmware, and switches that you plan to use in the configuration must be supported by the specific ONTAP version.

- **NetApp Interoperability**
  
  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.

- **NetApp Hardware Universe**

#### About this task

You must coordinate with the storage array administrator to perform this task on the storage array.

#### Steps

1. Create LUNs on the storage array depending on the number of nodes in the MetroCluster configuration.

   Each node in the MetroCluster configuration requires array LUNs for the root aggregate, data aggregate, and spares.

2. Configure parameters on the storage array that are required to work with ONTAP.

   - **FlexArray virtualization implementation for third-party storage**
   
   - **FlexArray virtualization implementation for NetApp E-Series storage**

#### Switch ports required for a MetroCluster configuration with array LUNs

When you are connecting ONTAP systems to FC switches for setting up a MetroCluster configuration with array LUNs, you must connect FC-VI and HBA ports from each controller to specific switch ports.

If you are using both array LUNs and disks in the MetroCluster configuration, you must ensure that the controller ports are connected to the switch ports recommended for configuration with disks, and then use the remaining ports for configuration with array LUNs.

The following table lists the specific FC switch ports to which you must connect the different controller ports in an eight-node MetroCluster configuration with array LUNs.
Overall cabling guidelines with array LUNs

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.

- 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.

- 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.

Brocade port usage for controllers in a MetroCluster configuration

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 on the Brocade 6510 and G620 switches.

Note: Port usage for the Brocade 6505 switch 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.

The following table shows the cabling for the first DR group:

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>3</td>
</tr>
</tbody>
</table>
## Brocade 6520, 6510, 6505, G620, G610, or 7840 switch

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>7</td>
</tr>
</tbody>
</table>

The following table shows the cabling for the second DR group:

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Brocade 6510</th>
<th>Brocade 6520</th>
<th>Brocade G620</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_3</td>
<td>FC-VI port a</td>
<td>24</td>
<td>-</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>24</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>25</td>
<td>-</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>25</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>26</td>
<td>-</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>26</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>27</td>
<td>-</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>27</td>
<td>-</td>
</tr>
<tr>
<td>controller_x_4</td>
<td>FC-VI port a</td>
<td>28</td>
<td>-</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>28</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>29</td>
<td>-</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>-</td>
<td>29</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>30</td>
<td>-</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>30</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>31</td>
<td>-</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>31</td>
<td>-</td>
</tr>
</tbody>
</table>

### ISLs

| ISL 1 | 40 | 40 | 23 | 23 | 40 | 40 |
### 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_1</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_2</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>
### Cisco 9396S

<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>

### Cisco 9148S

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</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_2</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>
### Cisco 9148S

<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>
</tbody>
</table>

### Cisco 9132T

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</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>
</tbody>
</table>
## Cisco 9132T

### MDS module 1

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_2</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>

### MDS module 2

<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>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>
<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>controller_x_1</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>HBA port a</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>6</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.

**Shared initiator and shared target support for MetroCluster configuration with array LUNs**

Being able to share a given FC initiator port or target ports is useful for organizations that want to minimize the number of initiator or target ports used. For example, an organization that expects low I/O usage over an FC initiator port or target ports might prefer to share FC initiator port or target ports instead of dedicating each FC initiator port to a single target port.

However sharing of initiator or target ports can adversely affect performance.

*NetApp Knowledgebase Answer 1030454: How to support Shared Initiator and Shared Target configuration with Array LUNs in a MetroCluster environment*
Cabling the FC-VI and HBA ports in a MetroCluster configuration with array LUNs

For a fabric-attached MetroCluster configuration with array LUNs, you must connect the controllers in a MetroCluster configuration to the storage arrays through FC switches.

Choices

• Cabling the FC-VI and HBA ports in a two-node fabric-attached MetroCluster configuration with array LUNs on page 243
• Cabling the FC-VI and HBA ports in a four-node fabric-attached MetroCluster configuration with array LUNs on page 244
• Cabling the FC-VI and HBA ports in an eight-node fabric-attached MetroCluster configuration with array LUNs on page 246

Cabling the FC-VI and HBA ports in a two-node fabric-attached MetroCluster configuration with array LUNs

If you are setting up a two-node fabric-attached MetroCluster configuration with array LUNs, you must cable the FC-VI ports and the HBA ports to the switch ports.

About this task

• You must repeat this task for each controller at both of the MetroCluster sites.
• If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the HBA ports and switch ports specified for configuration with disks.
  ◦ Port assignments for FC switches when using ONTAP 9.1 and later on page 52
  ◦ Port assignments for FC switches when using ONTAP 9.0 on page 37

Steps

1. Cable the FC-VI ports from the controller to alternate switch ports.
2. Perform the controller-to-switch cabling at both of the MetroCluster sites.

   You must ensure redundancy in connections from the controller to the switches. Therefore, for each controller at a site, you must ensure that both of the HBA ports in the same port pair are connected to alternate FC switches.

Example

The following example shows the connections between the HBA ports on Controller A and ports on FC_switch_A_1 and FC_switch_A_2:
The following table lists the connections between the HBA ports and the FC switch ports in the illustration:

<table>
<thead>
<tr>
<th>HBA ports</th>
<th>Switch ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port pair</td>
<td></td>
</tr>
<tr>
<td>Port a</td>
<td>FC_switch_A_1, Port 2</td>
</tr>
<tr>
<td>Port d</td>
<td>FC_switch_A_2, Port 3</td>
</tr>
<tr>
<td>Port pair</td>
<td></td>
</tr>
<tr>
<td>Port b</td>
<td>FC_switch_A_2, Port 2</td>
</tr>
<tr>
<td>Port c</td>
<td>FC_switch_A_1, Port 3</td>
</tr>
</tbody>
</table>

After you finish
You should cable the ISLs between the FC switches across the MetroCluster sites.

Cabling the FC-VI and HBA ports in a four-node fabric-attached MetroCluster configuration with array LUNs
If you are setting up a four-node fabric-attached MetroCluster configuration with array LUNs, you must cable the FC-VI ports and the HBA ports to the switch ports.

About this task
• You must repeat this task for each controller at both of the MetroCluster sites.
• If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the HBA ports and switch ports specified for configuration with disks.
  ◦ Port assignments for FC switches when using ONTAP 9.1 and later on page 52
  ◦ Port assignments for FC switches when using ONTAP 9.0 on page 37

Steps
1. Cable the FC-VI ports from each controller to the ports on alternate FC switches.

Example
The following example shows the connections between the FC-VI ports and switch ports at Site A:
2. Perform the controller-to-switch cabling at both of the MetroCluster sites.

You must ensure redundancy in connections from the controller to the switches. Therefore, for each controller at a site, you must ensure that both of the HBA ports in the same port pair are connected to alternate FC switches.

Example

The following example shows the connections between the HBA ports and switch ports at Site A:

The following table lists the connections between the HBA ports on controller_A_1 and the FC switch ports in the illustration:

<table>
<thead>
<tr>
<th>HBA ports</th>
<th>Switch ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port a</td>
<td>FC_switch_A_1, Port 2</td>
</tr>
<tr>
<td>Port d</td>
<td>FC_switch_A_2, Port 3</td>
</tr>
</tbody>
</table>
The following table lists the connections between the HBA ports on controller_A_2 and the FC switch ports in the illustration:

<table>
<thead>
<tr>
<th>HBA ports</th>
<th>Switch ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port pair</td>
<td></td>
</tr>
<tr>
<td>Port b</td>
<td>FC_switch_A_2, Port 2</td>
</tr>
<tr>
<td>Port c</td>
<td>FC_switch_A_1, Port 3</td>
</tr>
</tbody>
</table>

After you finish

You should cable the ISLs between the FC switches across the MetroCluster sites.

Related concepts

- **Switch ports required for a MetroCluster configuration with array LUNs** on page 235
- **Cabling the FC-VI and HBA ports in an eight-node fabric-attached MetroCluster configuration with array LUNs**

If you are setting up an eight-node fabric-attached MetroCluster configuration with array LUNs, you must cable the FC-VI ports and the HBA ports to the switch ports.

About this task

- You must repeat this task for each controller at both of the MetroCluster sites.
- If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the HBA ports and switch ports specified for configuration with disks.
  - *Port assignments for FC switches when using ONTAP 9.1 and later* on page 52
  - *Port assignments for FC switches when using ONTAP 9.0* on page 37

Step

1. Cable the FC-VI ports and HBA ports from each controller to the ports on alternate FC switches.
### Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

#### MetroCluster 1 or DR Group 1

<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>
<th>Connects to FC switch...</th>
<th>Connects to switch port...</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</td>
<td>FC-VI port a</td>
<td>1</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>1</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>2</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>FC-VI port c</td>
<td>1</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>FC-VI port d</td>
<td>2</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>1</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>2</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>1</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>2</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Stack 1</td>
<td>bridge_x_1a</td>
<td>FC1</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>bridge_x_1B</td>
<td>FC1</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Stack 2</td>
<td>bridge_x_2a</td>
<td>FC1</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>bridge_x_2B</td>
<td>FC1</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>Stack 3</td>
<td>bridge_x_3a</td>
<td>FC1</td>
<td>1</td>
<td>12*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>2</td>
<td>12*</td>
</tr>
<tr>
<td></td>
<td>bridge_x_3B</td>
<td>FC1</td>
<td>1</td>
<td>13*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC2</td>
<td>2</td>
<td>13*</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></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC_switch...</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.

## Cisco 9148 or 9250i*

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_x_1</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>HBA port a</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>controller_x_2</td>
<td>FC-VI port a</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FC-VI port b</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HBA port a</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port b</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>HBA port c</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>HBA port d</td>
<td>-</td>
<td>6</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>
</tbody>
</table>
### Cisco 9148 or 9250i*

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<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>

#### After you finish

You should cable the ISLs between the FC switches across the MetroCluster sites.

### Cabling the ISLs in a MetroCluster configuration with array LUNs

You must connect the FC switches across the sites through Inter-Switch Links (ISLs) to form switch fabrics in your MetroCluster configuration with array LUNs.

#### Step

1. Connect the switches at each site to the ISL or ISLs, using the cabling in the table that corresponds to your configuration and switch model.

The switch port numbers that you can use for the FC ISLs are as follows:

<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>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>Switch model</td>
<td>ISL port 1</td>
<td>Switch port</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Brocade 7840</td>
<td>ge0 (40-Gbps)</td>
<td>ISL port 2</td>
</tr>
<tr>
<td></td>
<td>ge2 (10-Gbps)</td>
<td>ISL port 3</td>
</tr>
<tr>
<td></td>
<td>ge1 (40-Gbps)</td>
<td>ISL port 4</td>
</tr>
<tr>
<td></td>
<td>ge3 (10-Gbps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ge10 (10-Gbps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ge11 (10-Gbps)</td>
<td></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>
<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</td>
<td>ISL 1</td>
<td>12</td>
</tr>
<tr>
<td>license or 9250i</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>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>
* The Cisco 9250i switch uses the FCIP ports for the ISL. There are certain limitations and procedures for using the FCIP ports.

*NetApp Knowledgebase Answer 1030474: How to configure the Cisco 9250i FC storage back end switch in MetroCluster for clustered Data ONTAP*

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

**Cabling the cluster interconnect in eight- or four-node configurations**

In eight- or four-node MetroCluster configurations, you must cable the cluster interconnect between the local controller modules at each site.

**About this task**

This task is not required on two-node MetroCluster configurations.

This task must be performed at both MetroCluster sites.

**Step**

1. Cable the cluster interconnect from one controller module to the other, or if cluster interconnect switches are used, from each controller module to the switches.

**Related information**

*AFF and FAS Documentation Center*

**Cabling the cluster peering connections**

You must cable the controller module ports used for cluster peering so that they have connectivity with the cluster on the partner site.

**About this task**

This task must be performed on each controller module in the MetroCluster configuration.

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.

**Related concepts**

*Considerations for configuring cluster peering* on page 10

**Related information**

*Cluster and SVM peering express configuration*
Cabling the HA interconnect, if necessary

If you have an eight- or a four-node MetroCluster configuration and the storage controllers within the HA pairs are in separate chassis, you must cable the HA interconnect between the controllers.

About this task

- This task does not apply to two-node MetroCluster configurations.
- This task must be performed at both MetroCluster sites.
- The HA interconnect must be cabled only if the storage controllers within the HA pair are in separate chassis.
  Some storage controller models support two controllers in a single chassis, in which case they use an internal HA interconnect.

Steps

1. Cable the HA interconnect if the storage controller's HA partner is in a separate chassis.

2. If the MetroCluster site includes two HA pairs, repeat the previous steps on the second HA pair.

3. Repeat this task at the MetroCluster partner site.

Cabling the management and data connections

You must cable the management and data ports on each storage controller to the site networks.

About this task

This task must be repeated for each new controller at both MetroCluster sites.

You can connect the controller and cluster switch management ports to existing switches in your network or to new dedicated network switches such as NetApp CN1601 cluster management switches.

Step

1. Cable the controller's management and data ports to the management and data networks at the local site.

Cabling storage arrays to FC switches in a MetroCluster configuration

You must connect storage arrays to FC switches so that the ONTAP systems in the MetroCluster configuration can access a specific array LUN through at least two paths.

Before you begin

- The storage arrays must be set up to present array LUNs to ONTAP.
- The ONTAP controllers must be connected to the FC switches.
- The ISLs must be cabled between the FC switches across the MetroCluster sites.

About this task

- You must repeat this task for each storage array at both of the MetroCluster sites.
• You must connect the controllers in a MetroCluster configuration to the storage arrays through FC switches.

**Step**

1. Connect the storage array ports to FC switch ports.
   At each site, connect the redundant port pairs in the storage array to FC switches on alternate fabrics. This provides redundancy in the paths for accessing the array LUNs.

**Related concepts**

*Switch zoning in a MetroCluster configuration with array LUNs* on page 256

**Related references**

*Example of cabling storage array ports to FC switches in a two-node MetroCluster configuration* on page 253

*Example of cabling storage array ports to FC switches in a four-node MetroCluster configuration* on page 254

*Example of cabling storage array ports to FC switches in an eight-node MetroCluster configuration* on page 256

**Example of cabling storage array ports to FC switches in a two-node MetroCluster configuration**

In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

The following illustration shows the connections between storage arrays and FC switches in a two-node fabric-attached MetroCluster configuration with array LUNs:

![Diagram of storage array and FC switch connections](image)

The connections between storage array ports and FC switch ports are similar for both stretch and fabric-attached variants of two-node MetroCluster configurations with array LUNs.

**Note:** If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the switch ports specified for the configuration with disks.

*Port assignments for FC switches when using ONTAP 9.1 and later* on page 52

In the illustration, the redundant array port pairs for both the sites are as follows:
• Storage array at Site A:
  ◦ Ports 1A and 2A
  ◦ Ports 1B and 2B

• Storage array at Site B:
  ◦ Ports 1A’ and 2A’
  ◦ Ports 1B’ and 2B’

FC_switch_A_1 at Site A and FC_switch_B_1 at Site B are connected to form fabric_1. Similarly, FC_switch_A_2 at Site A and FC_switch_B_2 are connected to form fabric_2.

The following table lists the connections between the storage array ports and the FC switches for the example MetroCluster illustration:

<table>
<thead>
<tr>
<th>Array LUN ports</th>
<th>FC switch ports</th>
<th>Switch fabrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site A</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1A</td>
<td>FC_switch_A_1, Port 9</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2A</td>
<td>FC_switch_A_2, Port 10</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1B</td>
<td>FC_switch_A_1, Port 10</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2B</td>
<td>FC_switch_A_2, Port 9</td>
<td>fabric_2</td>
</tr>
<tr>
<td><strong>Site B</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1A’</td>
<td>FC_switch_B_1, Port 9</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2A’</td>
<td>FC_switch_B_2, Port 10</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1B’</td>
<td>FC_switch_B_1, Port 10</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2B’</td>
<td>FC_switch_B_2, Port 9</td>
<td>fabric_2</td>
</tr>
</tbody>
</table>

**Example of cabling storage array ports to FC switches in a four-node MetroCluster configuration**

In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

The following reference illustration shows the connections between storage arrays and FC switches in a four-node MetroCluster configuration with array LUNs:
Note: If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the switch ports specified for the configuration with disks.

Port assignments for FC switches when using ONTAP 9.1 and later on page 52

In the illustration, the redundant array port pairs for both the sites are as follows:

- **Storage array at Site A:**
  - Ports 1A and 2A
  - Ports 1B and 2B
  - Ports 1C and 2C
  - Ports 1D and 2D

- **Storage array at Site B:**
  - Ports 1A’ and 2A’
  - Ports 1B’ and 2B’
  - Ports 1C’ and 2C’
  - Ports 1D’ and 2D’

FC_switch_A_1 at Site A and FC_switch_B_1 at Site B are connected to form fabric_1. Similarly, FC_switch_A_2 at Site A and FC_switch_B_2 are connected to form fabric_2.

The following table lists the connections between the storage array ports and the FC switches for the MetroCluster illustration:

<table>
<thead>
<tr>
<th>Array LUN ports</th>
<th>FC switch ports</th>
<th>Switch fabrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site A</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1A</td>
<td>FC_switch_A_1, Port 7</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2A</td>
<td>FC_switch_A_2, Port 11</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1B</td>
<td>FC_switch_A_1, Port 8</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2B</td>
<td>FC_switch_A_2, Port 10</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1C</td>
<td>FC_switch_A_1, Port 9</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2C</td>
<td>FC_switch_A_2, Port 9</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1D</td>
<td>FC_switch_A_1, Port 10</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2D</td>
<td>FC_switch_A_2, Port 8</td>
<td>fabric_2</td>
</tr>
<tr>
<td><strong>Site B</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1A’</td>
<td>FC_switch_B_1, Port 7</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2A’</td>
<td>FC_switch_B_2, Port 11</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1B’</td>
<td>FC_switch_B_1, Port 8</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2B’</td>
<td>FC_switch_B_2, Port 10</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1C’</td>
<td>FC_switch_B_1, Port 9</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2C’</td>
<td>FC_switch_B_2, Port 9</td>
<td>fabric_2</td>
</tr>
<tr>
<td>1D’</td>
<td>FC_switch_B_1, Port 10</td>
<td>fabric_1</td>
</tr>
<tr>
<td>2D’</td>
<td>FC_switch_B_2, Port 8</td>
<td>fabric_2</td>
</tr>
</tbody>
</table>
Example of cabling storage array ports to FC switches in an eight-node MetroCluster configuration

In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

An eight-node MetroCluster configuration consists of two four-node DR groups. The first DR group consists of the following nodes:

- controller_A_1
- controller_A_2
- controller_B_1
- controller_B_2

The second DR group consists of the following nodes:

- controller_A_3
- controller_A_4
- controller_B_3
- controller_B_4

To cable the array ports for the first DR group, you can use the cabling examples for a four-node MetroCluster configuration for the first DR group.

Example of cabling storage array ports to FC switches in a four-node MetroCluster configuration on page 254

To cable the array ports for the second DR group, follow the same examples and extrapolate for the FC-VI ports and FC initiator ports belonging to the controllers in the second DR group.

Switch zoning in a MetroCluster configuration with array LUNs

Configuring switch zoning enables you to define which array LUNs can be viewed by a specific ONTAP system in the MetroCluster configuration.

Related concepts

Example of switch zoning in a two-node MetroCluster configuration with array LUNs on page 257
Example of switch zoning in a four-node MetroCluster configuration with array LUNs on page 259
Example of switch zoning in an eight-node MetroCluster configuration with array LUNs on page 261

Requirements for switch zoning in a MetroCluster configuration with array LUNs

When using switch zoning in a MetroCluster configuration with array LUNs, you must ensure that certain basic requirements are followed.

The requirements for switch zoning in a MetroCluster configuration with array LUNs are as follows:

- The MetroCluster configuration must follow the single-initiator to single-target zoning scheme.
Single-initiator to single-target zoning limits each zone to a single FC initiator port and a single target port.

- The FC-VI ports must be zoned end-to-end across the fabric.
- Sharing of multiple initiator ports with a single target port can cause performance issues. Similarly, sharing of multiple target ports with a single initiator port can cause performance issues.
- You must have performed a basic configuration of the FC switches used in the MetroCluster configuration.

*Configuring the Cisco or Brocade FC switches manually* on page 72

**Shared initiator and shared target support for MetroCluster configuration with array LUNs**

Being able to share a given FC initiator port or target ports is useful for organizations that want to minimize the number of initiator or target ports used. For example, an organization that expects low I/O usage over an FC initiator port or target ports might prefer to share FC initiator port or target ports instead of dedicating each FC initiator port to a single target port.

However, sharing of initiator or target ports can adversely affect performance.

*NetApp Knowledgebase Answer 1030454: How to support Shared Initiator and Shared Target configuration with Array LUNs in a MetroCluster environment*

**Example of switch zoning in a two-node MetroCluster configuration with array LUNs**

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

You can use the following example as a reference when determining zoning for a two-node fabric-attached MetroCluster configuration with array LUNs:

The example shows single-initiator to single-target zoning for the MetroCluster configurations. The lines in the example represent zones rather than connections; each line is labeled with its zone number.

In the example, array LUNs are allocated on each storage array. LUNs of equal size are provisioned on the storage arrays at both sites, which is a SyncMirror requirement. Each ONTAP system has two paths to array LUNs. The ports on the storage array are redundant.
The redundant array port pairs for both the sites are as follows:

- **Storage array at Site A:**
  - Ports 1A and 2A
  - Ports 1B and 2B
- **Storage array at Site B:**
  - Ports 1A’ and 2A’
  - Ports 1B’ and 2B’

The redundant port pairs on each storage array form alternate paths. Therefore, both the ports of the port pairs can access the LUNs on the respective storage arrays.

The following table shows the zones for the illustrations:

<table>
<thead>
<tr>
<th>Zone</th>
<th>ONTAP controller and initiator port</th>
<th>Storage array port</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z1</td>
<td>Controller A: Port 0a</td>
<td>Port 1A</td>
</tr>
<tr>
<td>z3</td>
<td>Controller A: Port 0c</td>
<td>Port 1A’</td>
</tr>
<tr>
<td>FC_switch_A_2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z2</td>
<td>Controller A: Port 0b</td>
<td>Port 2A’</td>
</tr>
<tr>
<td>z4</td>
<td>Controller A: Port 0d</td>
<td>Port 2A</td>
</tr>
<tr>
<td>FC_switch_B_1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z5</td>
<td>Controller B: Port 0a</td>
<td>Port 1B’</td>
</tr>
<tr>
<td>z7</td>
<td>Controller B: Port 0c</td>
<td>Port 1B</td>
</tr>
<tr>
<td>FC_switch_B_2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z6</td>
<td>Controller B: Port 0b</td>
<td>Port 2B</td>
</tr>
<tr>
<td>z8</td>
<td>Controller B: Port 0d</td>
<td>Port 2B’</td>
</tr>
</tbody>
</table>

The following table shows the zones for the FC-VI connections:

<table>
<thead>
<tr>
<th>Zone</th>
<th>ONTAP controller and initiator port</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zX</td>
<td>Controller A: Port FC-VI a</td>
<td>FC_switch_A_1</td>
</tr>
<tr>
<td>zY</td>
<td>Controller A: Port FC-VI b</td>
<td>FC_switch_A_2</td>
</tr>
<tr>
<td>Site B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zX</td>
<td>Controller B: Port FC-VI a</td>
<td>FC_switch_B_1</td>
</tr>
<tr>
<td>zY</td>
<td>Controller B: Port FC-VI b</td>
<td>FC_switch_B_2</td>
</tr>
</tbody>
</table>
**Example of switch zoning in a four-node MetroCluster configuration with array LUNs**

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by a specific ONTAP systems.

You can use the following example as a reference when determining zoning for a four-node MetroCluster configuration with array LUNs. The example shows single-initiator to single-target zoning for a MetroCluster configuration. The lines in the following example represent zones rather than connections; each line is labeled with its zone number:

In the illustration, array LUNs are allocated on each storage array for the MetroCluster configuration. LUNs of equal size are provisioned on the storage arrays at both sites, which is a SyncMirror requirement. Each ONTAP system has two paths to array LUNs. The ports on the storage array are redundant.

In the illustration, the redundant array port pairs for both the sites are as follows:

- **Storage array at Site A:**
  - Ports 1A and 2A
  - Ports 1B and 2B
  - Ports 1C and 2C
  - Ports 1D and 2D

- **Storage array at Site B:**
  - Ports 1A’ and 2A’
  - Ports 1B’ and 2B’
  - Ports 1C’ and 2C’
  - Ports 1D’ and 2D’

The redundant port pairs on each storage array form alternate paths. Therefore, both the ports of the port pairs can access the LUNs on the respective storage arrays.

The following table shows the zones for this example:

<table>
<thead>
<tr>
<th>Zone</th>
<th>ONTAP controller and initiator port</th>
<th>Storage array port</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC_switch_A_1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td>ONTAP controller and initiator port</td>
<td>Storage array port</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>z1</td>
<td>Controller_A_1: Port 0a</td>
<td>Port 1A</td>
</tr>
<tr>
<td>z3</td>
<td>Controller_A_1: Port 0c</td>
<td>Port 1A'</td>
</tr>
<tr>
<td>z5</td>
<td>Controller_A_2: Port 0a</td>
<td>Port 1B</td>
</tr>
<tr>
<td>z7</td>
<td>Controller_A_2: Port 0c</td>
<td>Port 1B'</td>
</tr>
<tr>
<td></td>
<td><strong>FC_switch_A_2</strong></td>
<td></td>
</tr>
<tr>
<td>z2</td>
<td>Controller_A_1: Port 0b</td>
<td>Port 2A'</td>
</tr>
<tr>
<td>z4</td>
<td>Controller_A_1: Port 0d</td>
<td>Port 2A</td>
</tr>
<tr>
<td>z6</td>
<td>Controller_A_2: Port 0b</td>
<td>Port 2B'</td>
</tr>
<tr>
<td>z8</td>
<td>Controller_A_2: Port 0d</td>
<td>Port 2B</td>
</tr>
<tr>
<td></td>
<td><strong>FC_switch_B_1</strong></td>
<td></td>
</tr>
<tr>
<td>z9</td>
<td>Controller_B_1: Port 0a</td>
<td>Port 1C'</td>
</tr>
<tr>
<td>z11</td>
<td>Controller_B_1: Port 0c</td>
<td>Port 1C</td>
</tr>
<tr>
<td>z13</td>
<td>Controller_B_2: Port 0a</td>
<td>Port 1D'</td>
</tr>
<tr>
<td>z15</td>
<td>Controller_B_2: Port 0c</td>
<td>Port 1D</td>
</tr>
<tr>
<td></td>
<td><strong>FC_switch_B_2</strong></td>
<td></td>
</tr>
<tr>
<td>z10</td>
<td>Controller_B_1: Port 0b</td>
<td>Port 2C</td>
</tr>
<tr>
<td>z12</td>
<td>Controller_B_1: Port 0d</td>
<td>Port 2C'</td>
</tr>
<tr>
<td>z14</td>
<td>Controller_B_2: Port 0b</td>
<td>Port 2D</td>
</tr>
<tr>
<td>z16</td>
<td>Controller_B_2: Port 0d</td>
<td>Port 2D'</td>
</tr>
</tbody>
</table>

The following table shows the zones for the FC-VI connections at Site A and Site B:

<table>
<thead>
<tr>
<th>Zone</th>
<th>ONTAP controller and FC initiator port</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Site A</strong></td>
<td></td>
</tr>
<tr>
<td>zX</td>
<td>Controller_A_1: Port FC-VI a</td>
<td>FC_switch_A_1</td>
</tr>
<tr>
<td>zY</td>
<td>Controller_A_1: Port FC-VI b</td>
<td>FC_switch_A_2</td>
</tr>
<tr>
<td>zX</td>
<td>Controller_A_2: Port FC-VI a</td>
<td>FC_switch_A_1</td>
</tr>
<tr>
<td>zY</td>
<td>Controller_A_2: Port FC-VI b</td>
<td>FC_switch_A_2</td>
</tr>
<tr>
<td></td>
<td><strong>Site B</strong></td>
<td></td>
</tr>
<tr>
<td>zX</td>
<td>Controller_B_1: Port FC-VI a</td>
<td>FC_switch_B_1</td>
</tr>
<tr>
<td>zY</td>
<td>Controller_B_1: Port FC-VI b</td>
<td>FC_switch_B_2</td>
</tr>
<tr>
<td>zX</td>
<td>Controller_B_2: Port FC-VI a</td>
<td>FC_switch_B_1</td>
</tr>
<tr>
<td>zY</td>
<td>Controller_B_2: Port FC-VI b</td>
<td>FC_switch_B_2</td>
</tr>
</tbody>
</table>
Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

An eight-node MetroCluster configuration consists of two four-node DR groups. The first DR group consists of the following nodes:

- controller_A_1
- controller_A_2
- controller_B_1
- controller_B_2

The second DR group consists of the following nodes:

- controller_A_3
- controller_A_4
- controller_B_3
- controller_B_4

To configure the switch zoning, you can use the zoning examples for a four-node MetroCluster configuration for the first DR group.

*Example of switch zoning in a four-node MetroCluster configuration with array LUNs* on page 259

To configure zoning for the second DR group, follow the same examples and requirements for the FC initiator ports and array LUNs belonging to the controllers in the second DR group.

Setting up ONTAP in a MetroCluster configuration with array LUNs

After connecting the devices in the MetroCluster configuration, you must set up the ONTAP systems to use the storage on the storage array. You must also configure any required ONTAP feature.

Steps

1. Verifying and configuring the HA state of components in Maintenance mode on page 262
2. Configuring ONTAP on a system that uses only array LUNs on page 263
3. Setting up the cluster on page 266
4. Installing the license for using array LUNs in a MetroCluster configuration on page 266
5. Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems on page 267
6. Assigning ownership of array LUNs on page 268
7. Peering the clusters on page 269
8. Mirroring the root aggregates on page 269
9. Creating data aggregates on, implementing, and verifying the MetroCluster configuration on page 270
Verifying and configuring the HA state of components in Maintenance mode

When configuring a storage system in a MetroCluster configuration, you must make sure that the high-availability (HA) state of the controller module and chassis components is `mcc` or `mcc-2n` so that these components boot properly.

Before you begin

The system must be in Maintenance mode.

About this task

This task is not required on systems that are received from the factory.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:
   
   ```
   ha-config show
   ```
   
   The correct HA state depends on your MetroCluster configuration.

<table>
<thead>
<tr>
<th>Number of controllers in the MetroCluster configuration</th>
<th>HA state for all components should be...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eight- or four-node MetroCluster FC configuration</td>
<td>mcc</td>
</tr>
<tr>
<td>Two-node MetroCluster FC configuration</td>
<td>mcc-2n</td>
</tr>
<tr>
<td>MetroCluster IP configuration</td>
<td>mccip</td>
</tr>
</tbody>
</table>

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
   ```
   
   ```
   ha-config modify controller mcc-2n
   ```
   
   ```
   ha-config modify controller mccip
   ```

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

   ```
   ha-config modify chassis mcc
   ```
   
   ```
   ha-config modify chassis mcc-2n
   ```
   
   ```
   ha-config modify chassis mccip
   ```
4. Boot the node to ONTAP:
   `boot_ontap`

5. Repeat these steps on each node in the MetroCluster configuration.

**Configuring ONTAP on a system that uses only array LUNs**

If you want to configure ONTAP for use with array LUNs, you must configure the root aggregate and root volume, reserve space for diagnostics and recovery operations, and set up the cluster.

**Before you begin**

- The ONTAP system must be connected to the storage array.
- The storage array administrator must have created LUNs and presented them to ONTAP.
- The storage array administrator must have configured the LUN security.

**About this task**

You must configure each node that you want to use with array LUNs. If the node is in an HA pair, then you must complete the configuration process on one node before proceeding with the configuration on the partner node.

**Steps**

1. Power on the primary node and interrupt the boot process by pressing Ctrl-C when you see the following message on the console: Press CTRL-C for special boot menu.
2. Select option 4 (Clean configuration and initialize all disks) on the boot menu.

The list of array LUNs made available to ONTAP is displayed. In addition, the array LUN size required for root volume creation is also specified. The size required for root volume creation differs from one ONTAP system to another.

**Example**

- If no array LUNs were previously assigned, ONTAP detects and displays the available array LUNs, as shown in the following example:

```
mcc8040-ams1::> disk show NET-1.6 -instance
Disk: NET-1.6
Container Type: aggregate
Owner/Home: mcc8040-ams1-01 / mcc8040-ams1-01
DR Home: - / - / -
Stack ID/Shelf/Bay: - / - / -
LUN: 0
Array: NETAPP_INF_1
Vendor: NETAPP
Model: INF-01-00
Serial Number: 60080E50004317B4000003B158E35974
0000:00000000:00000000
BPS: 512
Physical Size: 87.50GB
Position: data
Checksum Compatibility: block
Aggregate: eseries
Plex: plex0
Paths: LUN Initiator Side Target Link
      Side Controller Initiator ID Switch Port Switch
```
If array LUNs were previously assigned, for example, through the maintenance mode, they are either marked local or partner in the list of the available array LUNs, depending on whether the array LUNs were selected from the node on which you are installing ONTAP or its HA partner:

In this example, array LUNs with index numbers 3 and 6 are marked local because they had been previously assigned from this particular node:

```
<table>
<thead>
<tr>
<th>Port</th>
<th>Acc Use</th>
<th>Target Port</th>
<th>TPGN</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcc8040-ams1-01</td>
<td>2c</td>
<td>mccb6505-ams1:16</td>
<td></td>
</tr>
<tr>
<td>mccb6505-ams1:18</td>
<td>AO</td>
<td>INU</td>
<td>20330080e54317b4</td>
</tr>
<tr>
<td>mcc8040-ams1-01</td>
<td>2a</td>
<td>mccb6505-ams1:17</td>
<td></td>
</tr>
<tr>
<td>mccb6505-ams1:19</td>
<td>ANO</td>
<td>RDY</td>
<td>20320080e54317b4</td>
</tr>
</tbody>
</table>

Speed | I/O KB/s | IOPS |
-------|---------|------|
-------|---------|------|
-------|---------|------|
-------|---------|------|

Errors:

- No disks are owned by this node, but array LUNs were assigned. You can use the following information to verify connectivity from HBAs to switch ports. If the connectivity of HBAs to switch ports does not match your expectations, configure your SAN and rescan. You can rescan by entering 'r' at the prompt for selecting array LUNs below.

HBA  HBA WWPN           Switch port      Switch port WWPN
---  --------           -----------      ----------------
0e  500a098001baf8e0  vgbr6510s203:25  20190027f88948dd
0f  500a098101baf8e0  vgci9710s202:1-17 2011547feeead680
0g  500a098201baf8e0  vgbr6510s203:27  201b0027f88948dd
0h  500a098301baf8e0  vgci9710s202:1-18 2012547feeead680

No native disks were detected, but array LUNs were detected. You will need to select an array LUN to be used to create the root aggregate and root volume.

Warning: The contents of the array LUN you select will be erased by ONTAP prior to their use.

Index  Array LUN Name       Model    Vendor   Size    Owner           Checksum  Serial Number
-----  ---------------------- -------- -------- -------- --------------  --------  ------------------------
0      vgci9710a20212-24.DL19  RAID5     DGC     217.3 GB  Block   6006016083402B0048E576D7
1      vgbr6510a203126.DL20  RAID5     DGC     217.3 GB  Block   6006016083402B0049E576D7
2      vgci9710a20212-24.DL21  RAID5     DGC     217.3 GB  Block   6006016083402B004AE576D7
3      vgbr6510a203126.DL22  RAID5     DGC     405.4 GB  local   Block   6006016083402B004BE576D7
4      vgci9710a20212-24.DL23  RAID5     DGC     217.3 GB  Block   6006016083402B004CE576D7
5      vgbr6510a203126.DL24  RAID5     DGC     217.3 GB  Block   6006016083402B004DE576D7
6      vgci9710a20212-24.DL25  RAID5     DGC     423.5 GB  local   Block   6006016083402B003CF93694
7      vgbr6510a203126.DL26  RAID5     DGC     423.5 GB  local   Block   6006016083402B003DF93694

Select the index number corresponding to the array LUN you want to assign as the root volume. The array LUN must be of sufficient size to create the root volume.

Example

In the following example, the array LUN with index number 3 is marked for root volume creation:

```
```

3. Select the index number corresponding to the array LUN you want to assign as the root volume.

The array LUN must be of sufficient size to create the root volume.

The array LUN selected for root volume creation is marked local (root).

Example

In the following example, the array LUN with index number 3 is marked for root volume creation:

```
```

The root volume will be created on switch 0:5.183L33.

ONTAP requires that 11.0 GB of space be reserved for use in diagnostic and recovery operations. Select one array LUN to be used as spare for diagnostic and recovery operations.

Index  Array LUN Name    Model       Vendor    Size   Owner           Checksum  Serial Number
-----  ----------------- ----------  ------  -------- --------------  --------  ------------------------
0      switch0:5.183L1  SYMMETRIX   EMC     266.1 GB  Block   60060480343613733416631
1      switch0:5.183L3  SYMMETRIX   EMC     266.1 GB  Block   60060480343613237643666
4. Select the index number corresponding to the array LUN you want to assign for use in diagnostic and recovery options.

The array LUN must be of sufficient size for use in diagnostic and recovery options. If required, you can also select multiple array LUNs with a combined size greater than or equal to the specified size. To select multiple entries, you must enter the comma-separated values of all of the index numbers corresponding to the array LUNs you want to select for diagnostic and recovery options.

Example

The following example shows a list of array LUNs selected for root volume creation and for diagnostic and recovery options:

<table>
<thead>
<tr>
<th>Index</th>
<th>Array LUN Name</th>
<th>Model</th>
<th>Vendor</th>
<th>Size</th>
<th>Owner</th>
<th>Checksum</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>switch0:5.183L31</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>266.1 GB</td>
<td>local</td>
<td>Block</td>
<td>600604803436313237643666</td>
</tr>
<tr>
<td>3</td>
<td>switch0:5.183L33</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>658.3 GB</td>
<td>local</td>
<td>Block</td>
<td>600604803436316263613066</td>
</tr>
<tr>
<td>4</td>
<td>switch0:7.183L0</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>173.6 GB</td>
<td>Block</td>
<td>Block</td>
<td>60060480343631261356235</td>
</tr>
<tr>
<td>5</td>
<td>switch0:7.183L2</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>173.6 GB</td>
<td>Block</td>
<td>Block</td>
<td>600604803436313237353738</td>
</tr>
<tr>
<td>6</td>
<td>switch0:7.183L4</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>658.3 GB</td>
<td>Block</td>
<td>Block</td>
<td>600604803436313161663031</td>
</tr>
<tr>
<td>7</td>
<td>switch0:7.183L30</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>173.6 GB</td>
<td>Block</td>
<td>Block</td>
<td>600604803436316538353834</td>
</tr>
<tr>
<td>8</td>
<td>switch0:7.183L32</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>266.1 GB</td>
<td>Block</td>
<td>Block</td>
<td>600604803436313237353738</td>
</tr>
<tr>
<td>9</td>
<td>switch0:7.183L34</td>
<td>SYMMETRIX</td>
<td>EMC</td>
<td>658.3 GB</td>
<td>Block</td>
<td>Block</td>
<td>600604803436313737333662</td>
</tr>
</tbody>
</table>

Note: Selecting “no” clears the LUN selection.

5. Enter y when prompted by the system to continue with the installation process.

The root aggregate and the root volume are created and the rest of the installation process continues.

6. Enter the required details to create the node management interface.

Example

The following example shows the node management interface screen with a message confirming the creation of the node management interface:

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.
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 192.0.2.66
Enter the node management interface netmask: 255.255.255.192
Enter the node management interface default gateway: 192.0.2.7
A node management interface on port e0M with IP address 192.0.2.66 has been created.
This node has its management address assigned and is ready for cluster setup.

After you finish

After configuring ONTAP on all of the nodes that you want to use with array LUNs, you should complete the cluster setup process.

Software setup

Related information

FlexArray virtualization installation requirements and reference
Setting up the cluster

Setting up the cluster involves setting up each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Related information

Software setup

Installing the license for using array LUNs in a MetroCluster configuration

You must install the V_StorageAttach license on each MetroCluster node that you want to use with array LUNs. You cannot use array LUNs in an aggregate until the license is installed.

Before you begin

- The cluster must be installed.
- You must have the license key for the V_StorageAttach license.

About this task

You must use a separate license key for each node on which you want to install the V_StorageAttach license.

Steps

1. Use the system license add command to install the V_StorageAttach license.
   
   Repeat this step for each cluster node on which you want to install the license.

2. Use the system license show command to verify that the V_StorageAttach license is installed on all required nodes in a cluster.

Example

The following sample output shows that the V_StorageAttach license is installed on the nodes of cluster_A:

```
cluster_A:~> system license show
Serial Number: nnnnnnnnnn
Owner: controller_A_1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
V_StorageAttach   license Virtual Attached Storage

Serial Number: llllllllll
Owner: controller_A_2
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
V_StorageAttach   license Virtual Attached Storage
```
Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems

If you are using the X1132A-R6 quad-port card on a FAS8020 system, you can enter Maintenance mode to configure the 1a and 1b ports for FC-VI and initiator usage. This is not required on MetroCluster systems received from the factory, in which the ports are set appropriately for your configuration.

About this task

This task must be performed in Maintenance mode.

Steps

1. Disable the ports:

   storage disable adapter 1a
   storage disable adapter 1b

   Example

   *> storage disable adapter 1a
   Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]:
   Offlining Fibre Channel adapter 1a.
   Host adapter 1a disable succeeded
   Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre
   Channel adapter 1a is now offline.
   *> storage disable adapter 1b
   Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]:
   Offlining Fibre Channel adapter 1b.
   Host adapter 1b disable succeeded
   Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre
   Channel adapter 1b is now offline.
   *

2. Verify that the ports are disabled:

   ucadmin show

   Example

   *> ucadmin show

   Adapter Current Current Pending Pending Admin
   Adapter Mode Type Mode Type Status
   ------- ------- -------- -------- -------
   ...     fc      initiator -   -    - offline
   1b fc    fc      initiator -   -    - online
   1c fc    fc      initiator -   -    - online
   1d fc    fc      initiator -   -    - online

3. Set the a and b ports to FC-VI mode:

   ucadmin modify -adapter 1a -type fcvi

   The command sets the mode on both ports in the port pair, 1a and 1b (even though only 1a is specified in the command).
Example

*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has changed to fcvi on adapter 1a. Reboot the controller for the changes to take effect.

*> ucadmin modify -t fcvi 1b
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has changed to fcvi on adapter 1b. Reboot the controller for the changes to take effect.

4. Confirm that the change is pending:

ucadmin show

Example

*> ucadmin show

<table>
<thead>
<tr>
<th>Adapter</th>
<th>Current Mode</th>
<th>Current Type</th>
<th>Pending Mode</th>
<th>Pending Type</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>lca</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>fcvi</td>
<td>offline</td>
</tr>
<tr>
<td>lcb</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>fcvi</td>
<td>offline</td>
</tr>
<tr>
<td>ldc</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>ldc</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>

5. Shut down the controller, and then reboot into Maintenance mode.

6. Confirm the configuration change:

ucadmin show local

Example

<table>
<thead>
<tr>
<th>Node</th>
<th>Adapter</th>
<th>Mode</th>
<th>Type</th>
<th>Mode</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_B_1</td>
<td>1a</td>
<td>fc</td>
<td>fcvi</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1b</td>
<td>fc</td>
<td>fcvi</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1c</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>1d</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>

6 entries were displayed.

Assigning ownership of array LUNs

Array LUNs must be owned by a node before they can be added to an aggregate to be used as storage.

Before you begin

- Back-end configuration testing (testing of the connectivity and configuration of devices behind the ONTAP systems) must be completed.
- Array LUNs that you want to assign must be presented to the ONTAP systems.
About this task

You can assign ownership of array LUNs that have the following characteristics:

- They are unowned.
- They have no storage array configuration errors, such as the following:
  - The array LUN is smaller than or larger than the size that ONTAP supports.
  - The LDEV is mapped on only one port.
  - The LDEV has inconsistent LUN IDs assigned to it.
  - The LUN is available on only one path.

ONTAP issues an error message if you try to assign ownership of an array LUN with back-end configuration errors that would interfere with the ONTAP system and the storage array operating together. You must fix such errors before you can proceed with array LUN assignment.

ONTAP alerts you if you try to assign an array LUN with a redundancy error: for example, all paths to this array LUN are connected to the same controller or only one path to the array LUN. You can fix a redundancy error before or after assigning ownership of the LUN.

Steps

1. Enter the following command to see the array LUNs that have not yet been assigned to a node:
   
   ```
   storage disk show -container-type unassigned
   ```

2. Enter the following command to assign an array LUN to this node:
   
   ```
   storage disk assign -disk arrayLUNname -owner nodename
   ```
   If you want to fix a redundancy error after disk assignment instead of before, you must use the `-force` parameter with the `storage disk assign` command.

Related information

* FlexArray virtualization installation requirements and reference

Peering the clusters

The clusters in the MetroCluster configuration must be in a peer relationship so that they can communicate with each other and perform the data mirroring essential to MetroCluster disaster recovery.

Steps

1. Configure intercluster LIFs using the procedure in Configuring intercluster LIFs on page 196.

2. Create a cluster peer relationship using the procedure in Creating a cluster peer relationship on page 200.

Mirroring the root aggregates

You must mirror the root aggregates in your MetroCluster configuration to ensure data protection.

Before you begin

You must have ensured that the SyncMirror requirements for the MetroCluster configuration with array LUNs are satisfied.

* Requirements for a MetroCluster configuration with array LUNs on page 233
About this task
You must repeat this task for each controller in the MetroCluster configuration.

Step
1. Use the `storage aggregate mirror` command to mirror the unmirrored root aggregate.

Example
The following command mirrors the root aggregate for controller_A_1:

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

The root aggregate is mirrored with array LUNs from pool1.

Creating data aggregates on, implementing, and verifying the MetroCluster configuration
You must create data aggregates on each node, implement, and verify the MetroCluster configuration.

Steps
1. Create data aggregates on each node:
   a. Create a mirrored data aggregate on each node using the procedure in Mirroring the root aggregates on page 269.
   b. If desired, create unmirrored data aggregates using the procedure in Creating a mirrored data aggregate on each node on page 204.

2. Implement the MetroCluster configuration using the procedure in Implementing the MetroCluster configuration on page 206.

3. Configure the MetroCluster FC switches for health monitoring using the procedure in Configuring the MetroCluster FC switches for health monitoring on page 212.

4. Check and verify the configuration:
   a. Check the MetroCluster configuration using the procedure in Checking the MetroCluster configuration on page 214.
   b. Check for MetroCluster configuration errors with Config Advisor using the procedure in Checking for MetroCluster configuration errors with Config Advisor on page 216.
   c. Verify switchover, healing, and switchback using the procedure in Verifying switchover, healing, and switchback on page 218.

5. Install the MetroCluster Tiebreaker software using the procedure in Installing the MetroCluster Tiebreaker software on page 218.

6. Set the destination for configuration backup files using the procedure in Protecting configuration backup files on page 218.
Implementing a MetroCluster configuration with both disks and array LUNs

To implement a MetroCluster configuration with native disks and array LUNs, you must ensure that the ONTAP systems used in the configuration can attach to storage arrays.

A MetroCluster configuration with disks and array LUNs can have either two or four nodes. Although the four-node MetroCluster configuration must be fabric-attached, the two-node configuration can either be stretch or fabric-attached.

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.

Related concepts

Example of a four-node MetroCluster configuration with disks and array LUNs on page 275

Related references

Example of a two-node fabric-attached MetroCluster configuration with disks and array LUNs on page 272

Considerations when implementing a MetroCluster configuration with disks and array LUNs

When planning your MetroCluster configuration for use with disks and array LUNs, you must consider various factors, such as the order of setting up access to storage, root aggregate location, and the usage of FC initiator ports, switches, and FC-to-SAS bridges.

Consider the information in the following table when planning your configuration:

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order of setting up access to the storage</td>
<td>You can set up access to either disks or array LUNs first. You must complete all setup for that type of storage and verify that it is set up correctly before setting up the other type of storage.</td>
</tr>
</tbody>
</table>
| Location of the root aggregate         | • If you are setting up a new MetroCluster deployment with both disks and array LUNs, you must create the root aggregate on native disks. When doing this, ensure that at least one disk shelf (with 24 disk drives) is set up at each of the sites.  
  • If you are adding native disks to an existing MetroCluster configuration that uses array LUNs, the root aggregate can remain on an array LUN. |
| Using switches and FC-to-SAS bridges    | FC-to-SAS bridges are required in four-node configurations and two-node fabric-attached configurations to connect the ONTAP systems to the disk shelves through the switches. You must use the same switches to connect to the storage arrays and the FC-to-SAS bridges. |
Using FC initiator ports

The initiator ports used to connect to an FC-to-SAS bridge must be different from the ports used to connect to the switches, which connect to the storage arrays. A minimum of eight initiator ports is required to connect an ONTAP system to both disks and array LUNs.

Related concepts

- Example of switch zoning in a four-node MetroCluster configuration with array LUNs on page 259
- Example of switch zoning in an eight-node MetroCluster configuration with array LUNs on page 261

Related tasks

- Configuring the Cisco or Brocade FC switches manually on page 72
- Installing FC-to-SAS bridges and SAS disk shelves on page 151

Related information

- NetApp Hardware Universe

Example of a two-node fabric-attached MetroCluster configuration with disks and array LUNs

For setting up a two-node fabric-attached MetroCluster configuration with native disks and array LUNs, you must use FC-to-SAS bridges to connect the ONTAP systems with the disk shelves through the FC switches. You can connect array LUNs through the FC switches to the ONTAP systems.

The following illustrations represent examples of a two-node fabric-attached MetroCluster configuration with disks and array LUNs. They both represent the same MetroCluster configuration; the representations for disks and array LUNs are separated only for simplification.

In the following illustration showing the connectivity between ONTAP systems and disks, the HBA ports 1a through 1d are used for connectivity with disks through the FC-to-SAS bridges:
In the following illustration showing the connectivity between ONTAP systems and array LUNs, the HBA ports 0a through 0d are used for connectivity with array LUNs because ports 1a through 1d are used for connectivity with disks:
Controller ports that connect to NetApp disk shelves
Example of a four-node MetroCluster configuration with disks and array LUNs

For setting up a four-node MetroCluster configuration with native disks and array LUNs, you must use FC-to-SAS bridges to connect the ONTAP systems with the disk shelves through the FC switches. You can connect array LUNs through the FC switches to the ONTAP systems.

A minimum of eight initiator ports is required for an ONTAP system to connect to both native disks and array LUNs.

The following illustrations represent examples of a MetroCluster configuration with disks and array LUNs. They both represent the same MetroCluster configuration; the representations for disks and array LUNs are separated only for simplification.

In the following illustration that shows the connectivity between ONTAP systems and disks, the HBA ports 1a through 1d are used for connectivity with disks through the FC-to-SAS bridges:
In the following illustration that shows the connectivity between ONTAP systems and array LUNs, the HBA ports 0a through 0d are used for connectivity with array LUNs because ports 1a through 1d are used for connectivity with disks:
Planning and installing a MetroCluster configuration with array LUNs

Site A
Controller_A_1
Controller_A_2
FC_switch_A_1
FC_switch_A_2
Array LUNS
Storage_array_1

Controller ports that connect to NetApp disk shelves
Using the Active IQ Unified Manager and ONTAP System Manager for further configuration and monitoring

The Active IQ Unified Manager and ONTAP System Manager can be used for GUI management of the clusters and monitoring of the configuration.

Each node has ONTAP System Manager pre-installed. To load System Manager, enter the cluster management LIF address as the URL in a web browser that has connectivity to the node.

You can also use Active IQ Unified Manager to monitor the MetroCluster configuration.

Related information

Active IQ Unified Manager and ONTAP System Manager Documentation

Synchronizing the system time using NTP

Each cluster needs its own Network Time Protocol (NTP) server to synchronize the time between the nodes and their clients. You can use the Edit DateTime dialog box in System Manager to configure the NTP server.

Before you begin

You must have downloaded and installed System Manager. System Manager is available from the NetApp Support Site.

About this task

• You cannot modify the time zone settings for a failed node or the partner node after a takeover occurs.

• Each cluster in the MetroCluster FC configuration should have its own separate NTP server or servers used by the nodes, FC switches, and FC-to-SAS bridges at that MetroCluster site.

   If you are using the MetroCluster Tiebreaker software, it should also have its own separate NTP server.

Steps

1. From the home page, double-click the appropriate storage system.

2. Expand the Cluster hierarchy in the left navigation pane.

3. In the navigation pane, click Configuration > System Tools > DateTime.

4. Click Edit.

5. Select the time zone.

6. Specify the IP addresses of the time servers, and then click Add.

   You must add an NTP server to the list of time servers. The domain controller can be an authoritative server.

7. Click OK.

8. Verify the changes you made to the date and time settings in the Date and Time window.
Considerations when using ONTAP in a MetroCluster configuration

When using ONTAP in a MetroCluster configuration, you should be aware of certain considerations for licensing, peering to clusters outside the MetroCluster configuration, performing volume operations, NVFAIL operations, and other ONTAP operations.

Licensing considerations

• Both sites should be licensed for the same site-licensed features.
• All nodes should be licensed for the same node-locked features.

SnapMirror consideration

• SnapMirror SVM disaster recovery is only supported on MetroCluster configurations running versions of ONTAP 9.5 or later.

FlexGroup support in MetroCluster configurations

Starting with ONTAP 9.6 MetroCluster configurations support FlexGroup volumes.

Job schedules in a MetroCluster configuration

In ONTAP 9.3 and later, user-created job schedules are automatically replicated between clusters in a MetroCluster configuration. If you create, modify, or delete a job schedule on a cluster, the same schedule is automatically created on the partner cluster, using Configuration Replication Service (CRS).

Note: System-created schedules are not replicated and you must manually perform the same operation on the partner cluster so that job schedules on both clusters are identical.

Cluster peering from the MetroCluster site to a third cluster

Because the peering configuration is not replicated, if you peer one of the clusters in the MetroCluster configuration to a third cluster outside of that configuration, you must also configure the peering on the partner MetroCluster cluster. This is so that peering can be maintained if a switchover occurs.

The non-MetroCluster cluster must be running ONTAP 8.3 or later. If not, peering is lost if a switchover occurs even if the peering has been configured on both MetroCluster partners.

LDAP client configuration replication in a MetroCluster configuration

An LDAP client configuration created on a storage virtual machine (SVM) on a local cluster is replicated to its partner data SVM on the remote cluster. For example, if the LDAP client configuration is created on the admin SVM on the local cluster, then it is replicated to all the admin data SVMs on the remote cluster. This MetroCluster feature is intentional so that the LDAP client configuration is active on all the partner SVMs on the remote cluster.
Networking and LIF creation guidelines for MetroCluster configurations

You should be aware of how LIFs are created and replicated in a MetroCluster configuration. You must also know about the requirement for consistency so that you can make proper decisions when configuring your network.

Related concepts

- [IPspace object replication and subnet configuration requirements on page 280](#)
- [Requirements for LIF creation in a MetroCluster configuration on page 281](#)
- [LIF replication and placement requirements and issues on page 281](#)

Related information

- [Network and LIF management](#)

IPspace object replication and subnet configuration requirements

You should be aware of the requirements for replicating IPspace objects to the partner cluster and for configuring subnets and IPv6 in a MetroCluster configuration.

IPspace replication

You must consider the following guidelines while replicating IPspace objects to the partner cluster:

- The IPspace names of the two sites must match.
- IPspace objects must be manually replicated to the partner cluster.
  Any storage virtual machines (SVMs) that are created and assigned to an IPspace before the IPspace is replicated will not be replicated to the partner cluster.

Subnet configuration

You must consider the following guidelines while configuring subnets in a MetroCluster configuration:

- Both clusters of the MetroCluster configuration must have a subnet in the same IPspace with the same subnet name, subnet, broadcast domain, and gateway.
- The IP ranges of the two clusters must be different.

In the following example, the IP ranges are different:

```
cluster_A::> network subnet show
IPspace: Default
Subnet Name                  Subnet               Broadcast Domain Gateway                   Avail/Total Ranges
--------- -------------------- ----------------- -------------- ----------------------- ------- -------
subnet1   192.168.2.0/24    Default            192.168.2.1     10/10
192.168.2.11-192.168.2.20
cluster_B::> network subnet show
IPspace: Default
Subnet Name                  Subnet               Broadcast Domain Gateway                   Avail/Total Ranges
--------- -------------------- ----------------- -------------- ----------------------- ------- -------
```
IPv6 configuration

If IPv6 is configured on one site, IPv6 must be configured on the other site as well.

Related concepts

Requirements for LIF creation in a MetroCluster configuration on page 281
LIF replication and placement requirements and issues on page 281

Requirements for LIF creation in a MetroCluster configuration

You should be aware of the requirements for creating LIFs when configuring your network in a MetroCluster configuration.

You must consider the following guidelines when creating LIFs:

• Fibre Channel: You must use stretched VSAN or stretched fabrics
• IP/iSCSI: You must use layer 2 stretched network
• ARP broadcasts: You must enable ARP broadcasts between the two clusters
• Duplicate LIFs: You must not create multiple LIFs with the same IP address (duplicate LIFs) in an IPspace

Verify LIF creation

You can confirm the successful creation of a LIF in a MetroCluster configuration by running the `metrocluster check lif show` command. If you encounter any issues while creating the LIF, you can use the `metrocluster check lif repair-placement` command to fix the issues.

Related concepts

IPspace object replication and subnet configuration requirements on page 280
LIF replication and placement requirements and issues on page 281

LIF replication and placement requirements and issues

You should be aware of the LIF replication requirements in a MetroCluster configuration. You should also know how a replicated LIF is placed on a partner cluster, and you should be aware of the issues that occur when LIF replication or LIF placement fails.

Replication of LIFs to the partner cluster

When you create a LIF on a cluster in a MetroCluster configuration, the LIF is replicated on the partner cluster. LIFs are not placed on a one-to-one name basis. For availability of LIFs after a switchover operation, the LIF placement process verifies that the ports are able to host the LIF based on reachability and port attribute checks.

The system must meet the following conditions to place the replicated LIFs on the partner cluster:
<table>
<thead>
<tr>
<th>Condition</th>
<th>LIF type: FC</th>
<th>LIF type: IP/iSCSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node identification</td>
<td>ONTAP attempts to place the replicated LIF on the disaster recovery (DR) partner of the node on which it was created. If the DR partner is unavailable, the DR auxiliary partner is used for placement.</td>
<td>ONTAP attempts to place the replicated LIF on the DR partner of the node on which it was created. If the DR partner is unavailable, the DR auxiliary partner is used for placement.</td>
</tr>
<tr>
<td>Port identification</td>
<td>ONTAP identifies the connected FC target ports on the DR cluster.</td>
<td>The ports on the DR cluster that are in the same IPspace as the source LIF are selected for a reachability check. If there are no ports in the DR cluster in the same IPspace, the LIF cannot be placed. All of the ports in the DR cluster that are already hosting a LIF in the same IPspace and subnet are automatically marked as reachable; and can be used for placement. These ports are not included in the reachability check.</td>
</tr>
<tr>
<td>Reachability check</td>
<td>Reachability is determined by checking for the connectivity of the source fabric WWN on the ports in the DR cluster. If the same fabric is not present at the DR site, the LIF is placed on a random port on the DR partner.</td>
<td>Reachability is determined by the response to an Address Resolution Protocol (ARP) broadcast from each previously identified port on the DR cluster to the source IP address of the LIF to be placed. For reachability checks to succeed, ARP broadcasts must be allowed between the two clusters. Each port that receives a response from the source LIF will be marked as possible for placement.</td>
</tr>
<tr>
<td>Condition</td>
<td>LIF type: FC</td>
<td>LIF type: IP/iSCSI</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port selection</td>
<td>ONTAP categorizes the ports based on attributes such as adapter type and speed, and then selects the ports with matching attributes. If no ports with matching attributes are found, the LIF is placed on a random connected port on the DR partner.</td>
<td>From the ports that are marked as reachable during the reachability check, ONTAP prefers ports that are in the broadcast domain that is associated with the subnet of the LIF. If there are no network ports available on the DR cluster that are in the broadcast domain that is associated with the subnet of the LIF, then ONTAP selects ports that have reachability to the source LIF. If there are no ports with reachability to the source LIF, a port is selected from the broadcast domain that is associated with the subnet of the source LIF, and if no such broadcast domain exists, a random port is selected. ONTAP categorizes the ports based on attributes such as adapter type, interface type, and speed, and then selects the ports with matching attributes.</td>
</tr>
<tr>
<td>LIF placement</td>
<td>From the reachable ports, ONTAP selects the least loaded port for placement.</td>
<td>From the selected ports, ONTAP selects the least loaded port for placement.</td>
</tr>
</tbody>
</table>

**Placement of replicated LIFs when the DR partner node is down**

When an iSCSI or FC LIF is created on a node whose DR partner has been taken over, the replicated LIF is placed on the DR auxiliary partner node. After a subsequent giveback operation, the LIFs are not automatically moved to the DR partner. This can lead to LIFs being concentrated on a single node in the partner cluster. During a MetroCluster switchover operation, subsequent attempts to map LUNs belonging to the storage virtual machine (SVM) fail.

You should run the `metrocluster check lif show` command after a takeover operation or giveback operation to verify that the LIF placement is correct. If errors exist, you can run the `metrocluster check lif repair-placement` command to resolve the issues.

**LIF placement errors**

LIF placement errors that are displayed by the `metrocluster check lif show` command are retained after a switchover operation. If the `network interface modify`, `network interface rename`, or `network interface delete` command is issued for a LIF with a placement error, the error is removed and does not appear in the output of the `metrocluster check lif show` command.
LIF replication failure

You can also check whether LIF replication was successful by using the `metrocluster check lif show` command. An EMS message is displayed if LIF replication fails.

You can correct a replication failure by running the `metrocluster check lif repair-placement` command for any LIF that fails to find a correct port. You should resolve any LIF replication failures as soon as possible to verify the availability of LIF during a MetroCluster switchover operation.

**Note:** Even if the source SVM is down, LIF placement might proceed normally if there is a LIF belonging to a different SVM in a port with the same IPspace and network in the destination SVM.

LIFs inaccessible after a switchover

If any change is made in the FC switch fabric to which the FC target ports of the source and DR nodes are connected, then the FC LIFs that are placed at the DR partner might become inaccessible to the hosts after a switchover operation.

You should run the `metrocluster check lif repair-placement` command on the source as well as the DR nodes after a change is made in the FC switch fabric to verify the host connectivity of LIFs. The changes in the switch fabric might result in LIFs getting placed in different target FC ports at the DR partner node.

Related concepts

- *IPspace object replication and subnet configuration requirements* on page 280
- *Requirements for LIF creation in a MetroCluster configuration* on page 281

Volume creation on a root aggregate

The system does not allow the creation of new volumes on the root aggregate (an aggregate with an HA policy of CFO) of a node in a MetroCluster configuration.

Because of this restriction, root aggregates cannot be added to an SVM using the `vserver add-aggregates` command.

SVM disaster recovery in a MetroCluster configuration

Starting with ONTAP 9.5, active storage virtual machines (SVMs) in a MetroCluster configuration can be used as sources with the SnapMirror SVM disaster recovery feature. The destination SVM must be on the third cluster outside of the MetroCluster configuration.

You should be aware of the following requirements and limitations of using SVMs with SnapMirror disaster recovery:

- Only an active SVM within a MetroCluster configuration can be the source of an SVM disaster recovery relationship. A source can be a sync-source SVM before switchover or a sync-destination SVM after switchover.

- When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM disaster recovery relationship, since the volumes are not online. The following image shows the SVM disaster recovery behavior in a steady state:
• When the sync-source SVM is the source of an SVM DR relationship, the source SVM DR relationship information is replicated to the MetroCluster partner. This enables the SVM DR updates to continue after a switchover as shown in the following image:

• During the switchover and switchback processes, replication to the SVM DR destination might fail. However, after the switchover or switchback process completes, the next SVM DR scheduled updates will succeed.

See the section “Replicating the SVM configuration” in the *Data Protection Power Guide* for details on configuring an SVM DR relationship.

*Data protection*
SVM resynchronization at a disaster recovery site

During resynchronization, the storage virtual machines (SVMs) disaster recovery (DR) source on the MetroCluster configuration is restored from the destination SVM on the non-MetroCluster site.

During resynchronization, the source SVM (cluster_A) temporarily acts as a destination SVM as shown in the following image:

![Image of MetroCluster configuration with SVMs and SnapMirror relationship]

If an unplanned switchover occurs during resynchronization

Unplanned switchovers that occur during the resynchronization will halt the resynchronization transfer. If an unplanned switchover occurs, the following conditions are true:

- The destination SVM on the MetroCluster site (which was a source SVM prior to resynchronization) remains as a destination SVM. The SVM at the partner cluster will continue to retain its subtype and remain inactive.
- The SnapMirror relationship must be re-created manually with the sync-destination SVM as the destination.
- The SnapMirror relationship does not appear in the SnapMirror show output after a switchover at the survivor site unless a SnapMirror create operation is executed.

Performing switchback after an unplanned switchover during resynchronization

To successfully perform the switchback process, the resynchronization relationship must be broken and deleted. Switchback is not permitted if there are any SnapMirror DR destination SVMs in the MetroCluster configuration or if the cluster has an SVM of subtype “dp-destination”.

Output for the storage aggregate plex show command is indeterminate after a MetroCluster switchover

When you run the `storage aggregate plex show` command after a MetroCluster switchover, the status of plex0 of the switched over root aggregate is indeterminate and is displayed as `failed`. 
During this time, the switched over root is not updated. The actual status of this plex can only be determined after the MetroCluster healing phase.

**Modifying volumes to set the NVFAIL flag in case of switchover**

You can modify a volume so that the NVFAIL flag is set on the volume in the event of a MetroCluster switchover. The NVFAIL flag causes the volume to be fenced off from any modification. This is required for volumes that need to be handled as if committed writes to the volume were lost after the switchover.

**About this task**

*Note:* In ONTAP versions earlier than 9.0, the NVFAIL flag is used for each switchover. In ONTAP 9.0 and later versions, the unplanned switchover (USO) is used.

**Step**

1. Enable MetroCluster configuration to trigger NVFAIL on switchover by setting the `vol -dr-force-nvfail` parameter to `on`:

   ```bash
   vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
   ```

**Monitoring and protecting the file system consistency using NVFAIL**

The `-nvfail` parameter of the `volume modify` command enables ONTAP to detect nonvolatile RAM (NVRAM) inconsistencies when the system is booting or after a switchover operation. It also warns you and protects the system against data access and modification until the volume can be manually recovered.

If ONTAP detects any problems, database or file system instances stop responding or shut down. ONTAP then sends error messages to the console to alert you to check the state of the database or file system. You can enable NVFAIL to warn database administrators of NVRAM inconsistencies among clustered nodes that can compromise database validity.

After the NVRAM data loss during failover or boot recovery, NFS clients cannot access data from any of the nodes until the NVFAIL state is cleared. CIFS clients are unaffected.

**How NVFAIL impacts access to NFS volumes or LUNs**

The NVFAIL state is set when ONTAP detects NVRAM errors when booting, when a MetroCluster switchover operation occurs, or during an HA takeover operation if the NVFAIL option is set on the volume. If no errors are detected at startup, the file service is started normally. However, if NVRAM errors are detected or NVFAIL processing is enforced on a disaster switchover, ONTAP stops database instances from responding.

When you enable the NVFAIL option, one of the processes described in the following table takes place during bootup:

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP detects no NVRAM errors</td>
<td>File service starts normally.</td>
</tr>
</tbody>
</table>
If... | Then...
---|---
ONTAP detects NVRAM errors | • ONTAP returns a stale file handle (\texttt{ESTALE}) error to NFS clients trying to access the database, causing the application to stop responding, crash, or shut down. ONTAP then sends an error message to the system console and log file.
• When the application restarts, files are available to CIFS clients even if you have not verified that they are valid. For NFS clients, files remain inaccessible until you reset the \texttt{in-nvfailed-state} option on the affected volume.

If one of the following parameters is used:  
• \texttt{dr-force-nvfail} volume option is set  
• \texttt{force-nvfail-all} switchover command option is set. | You can unset the \texttt{dr-force-nvfail} option after the switchover, if the administrator is not expecting to force NVFAIL processing for possible future disaster switchover operations. For NFS clients, files remain inaccessible until you reset the \texttt{in-nvfailed-state} option on the affected volume.  
\textbf{Note:} Using the \texttt{force-nvfail-all} option causes the \texttt{dr-force-nvfail} option to be set on all of the DR volumes processed during the disaster switchover.

ONTAP detects NVRAM errors on a volume that contains LUNs | LUNs in that volume are brought offline. The \texttt{in-nvfailed-state} option on the volume must be cleared, and the \texttt{NVFAIL} attribute on the LUNs must be cleared by bringing each LUN in the affected volume online.
You can perform the steps to check the integrity of the LUNs and recover the LUN from a Snapshot copy or back up as necessary. After all of the LUNs in the volume are recovered, the \texttt{in-nvfailed-state} option on the affected volume is cleared.

\section*{Commands for monitoring data loss events}

If you enable the \texttt{NVFAIL} option, you receive notification when a system crash caused by NVRAM inconsistencies or a MetroCluster switchover occurs.

By default, the NVFAIL parameter is not enabled.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new volume with NVFAIL enabled</td>
<td>\texttt{volume create -nvfail on}</td>
</tr>
</tbody>
</table>
| Enable NVFAIL on an existing volume | \texttt{volume modify}  
\textbf{Note:} You set the \texttt{-nvfail} option to \texttt{on} to enable NVFAIL on the created volume. |
If you want to... | Use this command...
---|---
Display whether NVFAIL is currently enabled for a specified volume | `volume show`

**Note:** You set the `-fields` parameter to `nvfail` to display the NVFAIL attribute for a specified volume.

See the man page for each command for more information.

**Accessing volumes in NVFAIL state after a switchover**

After a switchover, you must clear the NVFAIL state by resetting the `-in-nvfailed-state` parameter of the `volume modify` command to remove the restriction of clients to access data.

**Before you begin**
The database or file system must not be running or trying to access the affected volume.

**About this task**
Setting `-in-nvfailed-state` parameter requires advanced-level privilege.

**Step**
1. Recover the volume by using the `volume modify` command with the `-in-nvfailed-state` parameter set to `false`.

**After you finish**
For instructions about examining database file validity, see the documentation for your specific database software.
If your database uses LUNs, review the steps to make the LUNs accessible to the host after an NVRAM failure.

**Recovering LUNs in NVFAIL states after switchover**

After a switchover, the host no longer has access to data on the LUNs that are in NVFAIL states. You must perform a number of actions before the database has access to the LUNs.

**Before you begin**
The database must not be running.

**Steps**
1. Clear the NVFAIL state on the affect volume that hosts the LUNs by resetting the `-in-nvfailed-state` parameter of the `volume modify` command.
2. Bring the affected LUNs online.
3. Examine the LUNs for any data inconsistencies and resolve them.
   This might involve host-based recovery or recovery done on the storage controller using SnapRestore.
4. Bring the database application online after recovering the LUNs.
Where to find additional information

You can learn more about MetroCluster configuration and operation from the NetApp 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>
</tbody>
</table>
  • Best practices for MetroCluster FC configuration. |
| **Stretch MetroCluster installation and configuration** | • Stretch MetroCluster architecture                                   
  • Cabling the configuration                       
  • Configuring the FC-to-SAS bridges                
  • Configuring the MetroCluster in ONTAP            |
| **MetroCluster IP installation and configuration** | • MetroCluster IP architecture                                        
  • Cabling the configuration                        
  • Configuring the MetroCluster in ONTAP            |
| **MetroCluster management and disaster recovery** | • Understanding the MetroCluster configuration                          
  • Switchover, healing and switchback               
  • Disaster recovery                                 |
<table>
<thead>
<tr>
<th>Guide</th>
<th>Content</th>
</tr>
</thead>
</table>
| **MetroCluster Service Guide**                                       | • Guidelines for maintenance in a MetroCluster FC configuration  
• Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches  
• Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration  
• Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration  
• Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration  
• Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration.  
• Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration. |
| **MetroCluster Tiebreaker Software Installation and Configuration Guide** | • Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software                                                                 |
| Active IQ Unified Manager documentation                              | • Monitoring the MetroCluster configuration and performance                                                                                                                                     |
| **NetApp Documentation: Product Guides and Resources**               |                                                                                                                                                                                                  |
| **Copy-based transition**                                            | • Transitioning data from 7-Mode storage systems to clustered storage systems                                                                                                                   |
| **ONTAP concepts**                                                   | • How mirrored aggregates work                                                                                                                                                                  |
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