Cabling a fabric-attached MetroCluster configuration

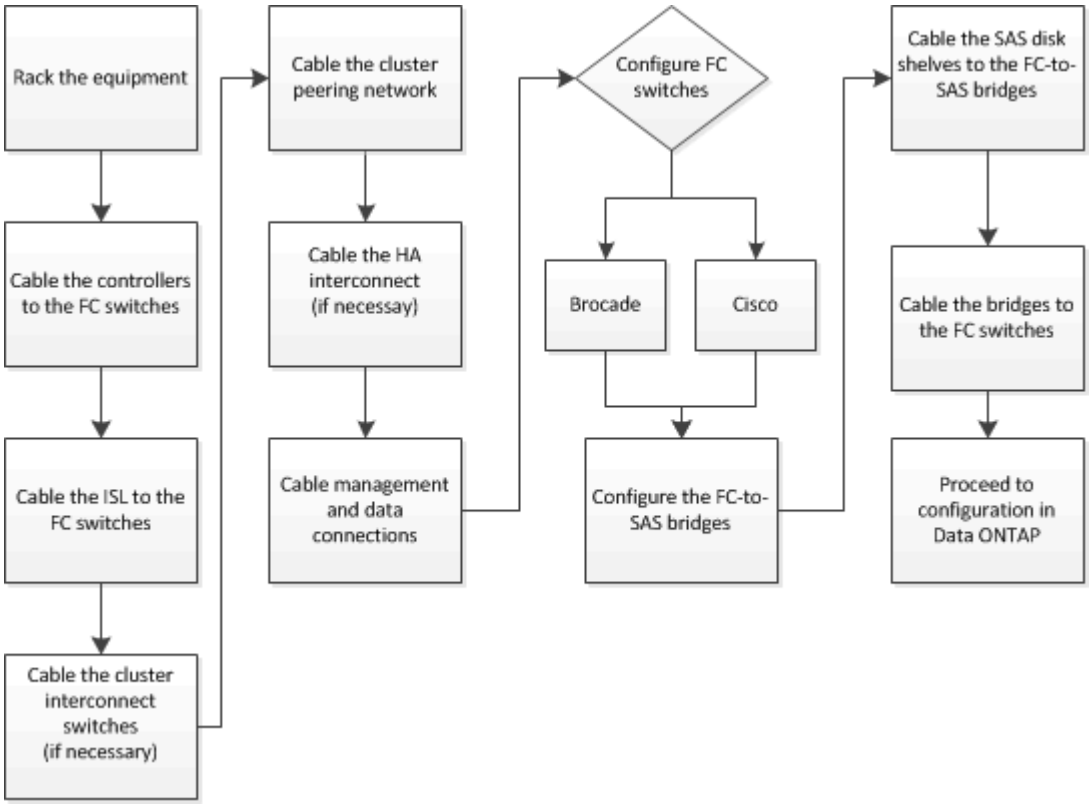
ONTAP MetroCluster

NetApp
April 28, 2021

Table of Contents

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.



Parts of a fabric MetroCluster configuration

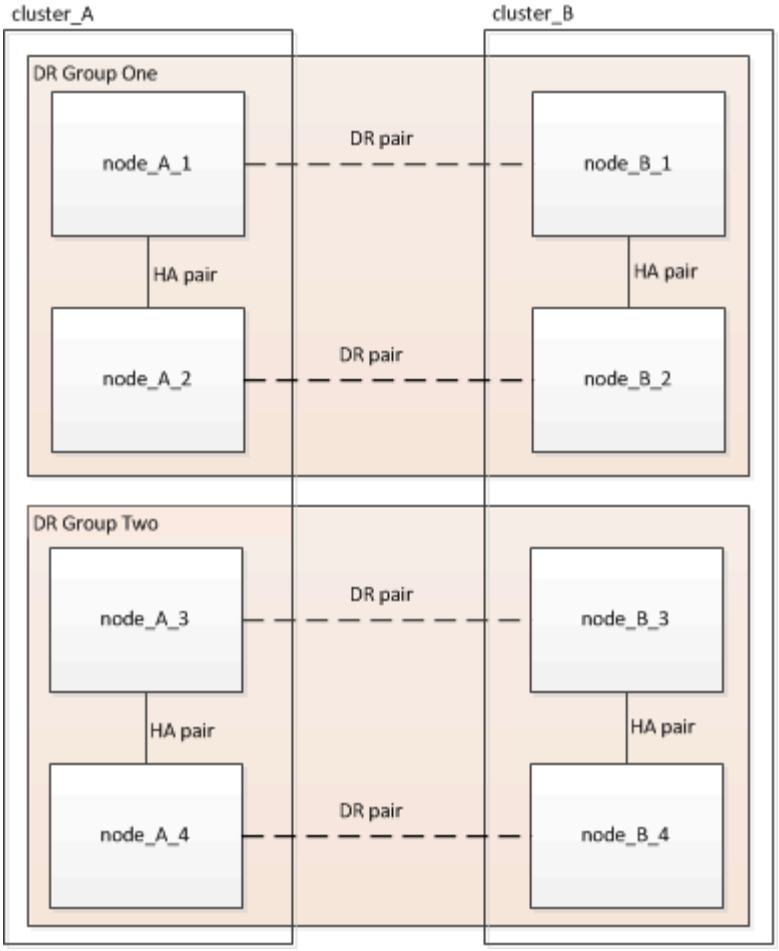
As you plan your MetroCluster configuration, you should understand the hardware components and how they interconnect.

Disaster Recovery (DR) groups

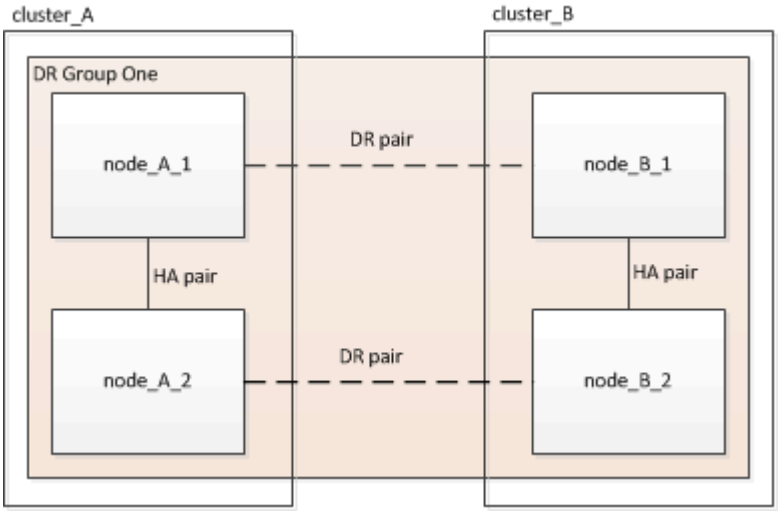
A fabric MetroCluster configuration consists of one or two DR groups, depending on the number of nodes in the MetroCluster configuration. Each DR group consists of four nodes.

- 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:



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.

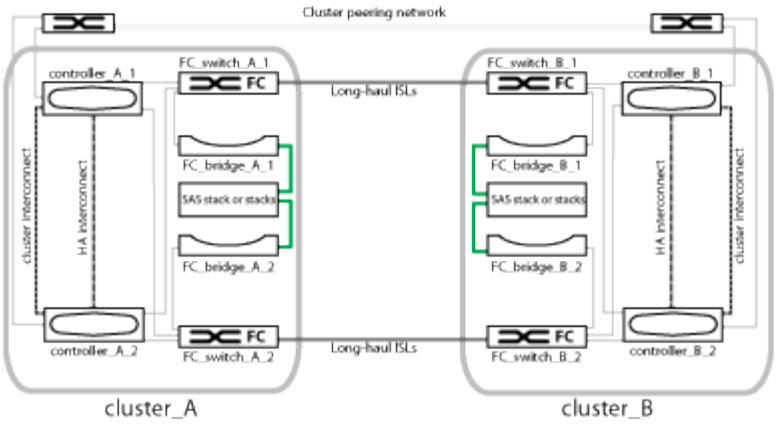
- Ethernet connections from the controllers to the customer-provided network that is used for cluster peering

  SVM configuration is replicated over the cluster peering network.

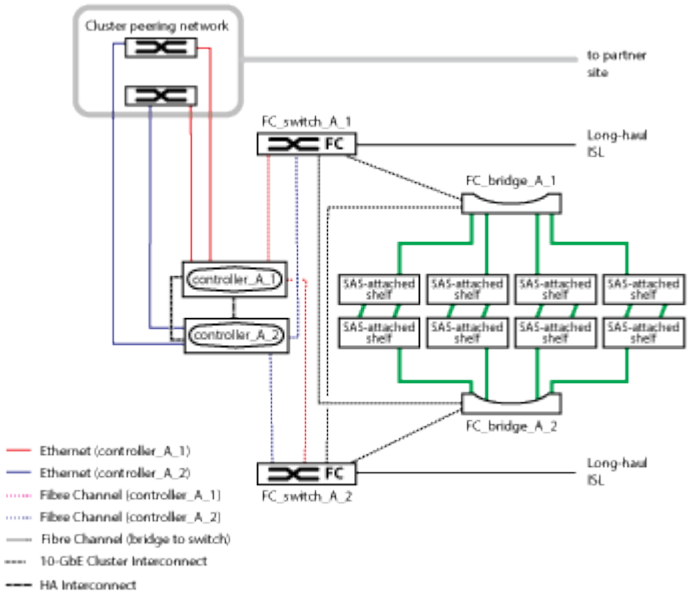
- A cluster interconnect between each controller in the local cluster

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.

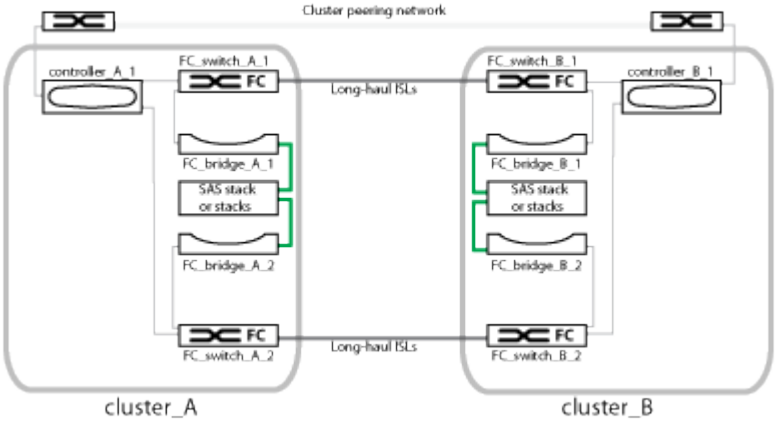


The following illustration shows a more detailed view of the connectivity in a single MetroCluster cluster (both clusters have the same configuration):



Two-node fabric MetroCluster configuration

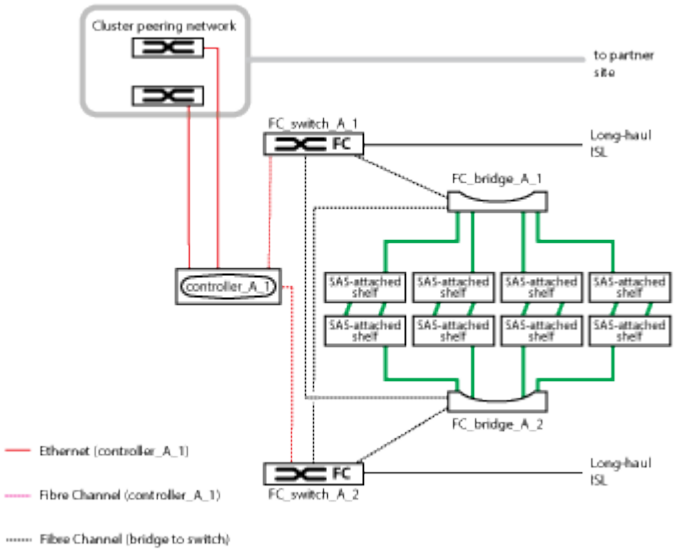
The following illustration shows a simplified view of a two-node fabric MetroCluster configuration. For some connections, a single line represents multiple, redundant connections between the components. Data and management network connections are not shown.



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.

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:

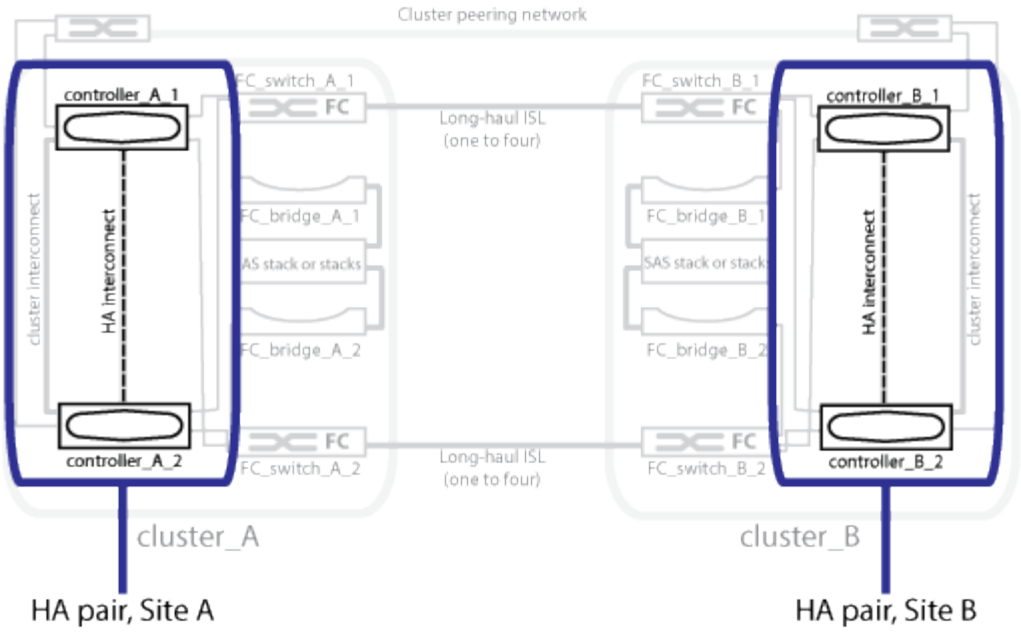
- FC connections between the FC-VI adapter on each controller module
- FC connections from each controller module's HBAs to the FC-to-SAS bridge for each SAS shelf stack
- SAS connections between each SAS shelf and from the top and bottom of each stack to an FC-to-SAS bridge
- Ethernet connections from 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.



Related information

Illustration of redundant FC-to-SAS bridges

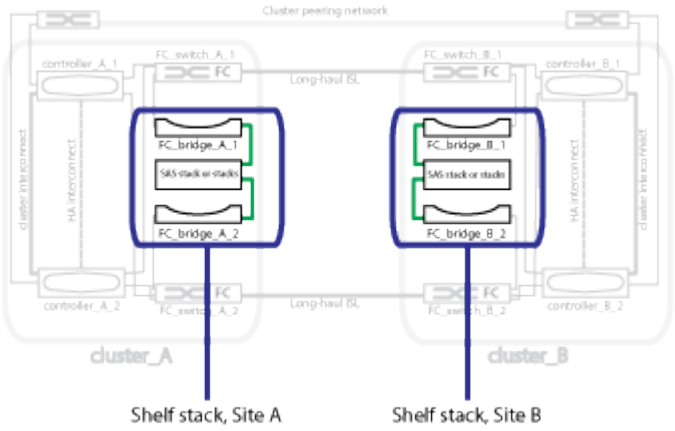
Redundant FC switch fabrics

Illustration of the cluster peering network

ONTAP concepts

Illustration of redundant FC-to-SAS bridges

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



Related information

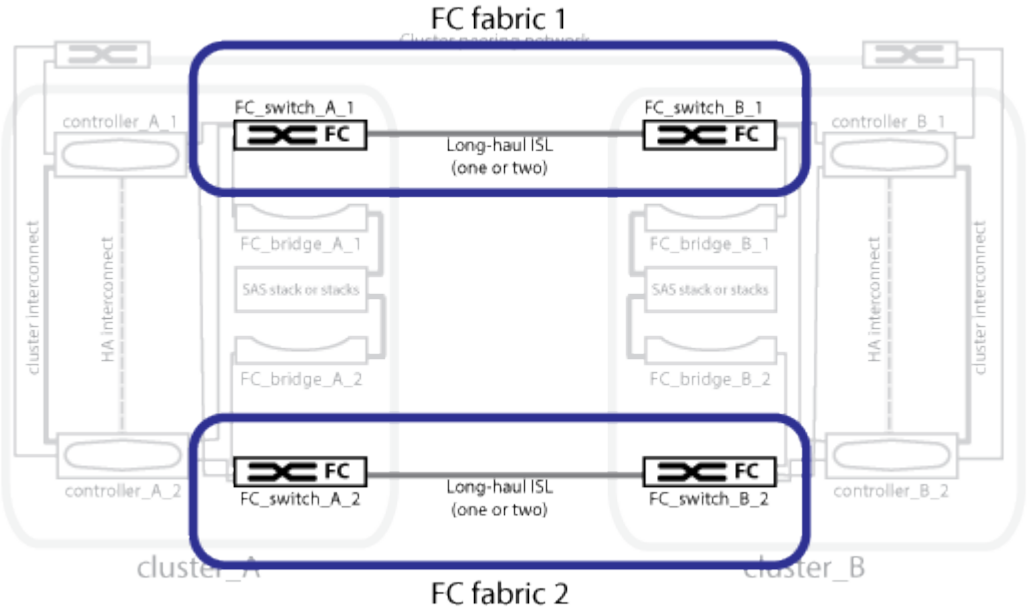
Illustration of the local HA pairs in a MetroCluster configuration

Redundant FC switch fabrics

Illustration of the cluster peering network

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.



Related information

Illustration of the local HA pairs in a MetroCluster configuration

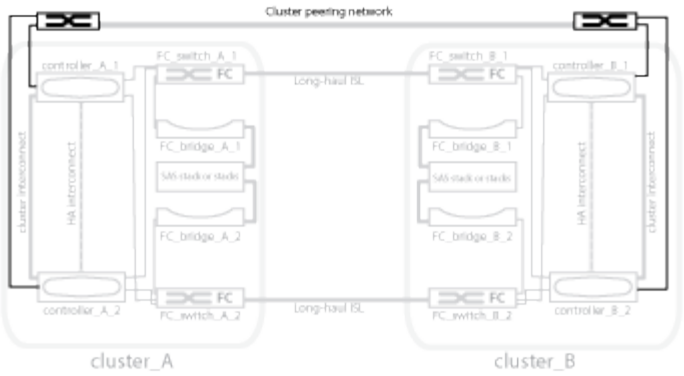
Illustration of redundant FC-to-SAS bridges

Illustration of the cluster peering network

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 information

Illustration of the local HA pairs in a MetroCluster configuration

Illustration of redundant FC-to-SAS bridges

Redundant FC switch fabrics

Cluster and SVM peering express configuration

Considerations for configuring cluster peering

Cabling the cluster peering connections

Peering the clusters

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.

Long-wave SFPs are not supported in the MetroCluster storage switches. For a table of supported SPFs, 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 6500N bridges are not supported in configurations running ONTAP 9.8 and later.

- 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 IOM3 modules is not supported within the same storage stack. A mix of IOM12 modules and IOM6 modules is supported within the same storage stack if your system is running a supported version of ONTAP.

  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 24 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

In a minimum supported configuration, at least one shelf is needed per site.

MetroCluster configurations support RAID-DP and RAID4.

Drive location considerations for partially populated shelves

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.

In a configuration with a partially populated shelf, the drives must be evenly distributed in the four quadrants of the shelf.

Mixing IOM12 and IOM 6 modules in a stack

Your version of ONTAP must support shelf mixing. Refer to the Interoperability Matrix Tool (IMT) to see if your version of ONTAP supports shelf mixing. NetApp Interoperability

For further details on shelf mixing see: Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules

Bridge naming conventions

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

This portion of the name…	Identifies the…	Possible values…
site	Site on which the bridge pair physically resides.	A or B
stack group	Number of the stack group to which the bridge pair connects. • 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. • FibreBridge 6500N bridges support only a single stack in the stack group.	1, 2, etc.
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

Configuration worksheets for FC switches and FC-to-SAS bridges

Before beginning to configure the MetroCluster sites, you can use the following worksheets to record your site information:

Site A worksheet

Site B worksheet

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.

Racking the hardware components

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

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.

   AFF and FAS Documentation Center

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.

   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.

   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.

Steps

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

Cabling the 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.

This must be done for both switch fabrics.

Steps

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 FC switches when using ONTAP 9.1 and later
   - Port assignments for FC switches when using ONTAP 9.0

Related information

Considerations for ISLs

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 Maintenance Guide*.

MetroCluster Maintenance Guide

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

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only			
MetroCluster 1 or DR Group 1			
Component	Port	Brocade switch models 6505, 6510, 6520, 7840, G620, G610, and DCX 8510-8	
		Connects to FC switch…	Connects to switch port…
controller_x_1	FC-VI port a	1	0
	FC-VI port b	2	0
	FC-VI port c	1	1
	FC-VI port d	2	1
	HBA port a	1	2
	HBA port b	2	2
	HBA port c	-	-
	HBA port d	-	-

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only			
Stack 1	bridge_x_1a	1	8
	bridge_x_1b	2	8
Stack y	bridge_x_ya	1	11
	bridge_x_yb	2	11

The following table shows port assignments for FC switches when using ONTAP 9.0.

MetroCluster two-node configuration			
Component	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

Port assignments for FC switches when using ONTAP 9.0

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later versions of ONTAP.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCF files are used, ISL ports may not connect to the same ports shown here and may need to be reconfigured manually.

Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.

    - On Cisco switches, the first port is numbered 1.
- The cabling is the same for each FC switch in the switch fabric.
- AFF A300 and FAS8200 storage systems can be ordered with one of two options for FC-VI connectivity:
    - Onboard ports 0e and 0f configured in FC-VI mode.
    - Ports 1a and 1b on an FC-VI card in slot 1.

Brocade port usage for controller connections in an eight-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Brocade switches:

MetroCluster eight-node configuration			
Component	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2
controller_x_2	FC-VI port a	3	-
	FC-VI port b	-	3
	HBA port a	4	-
	HBA port b	-	4
	HBA port c	5	-
	HBA port d	-	5
controller_x_3	FC-VI port a	6	
FC-VI port b	-	6	HBA port a

MetroCluster eight-node configuration			
7	-	HBA port b	-
7	HBA port c	8	-
HBA port d	-	8	controller_x_4
FC-VI port a	9	-	FC-VI port b
-	9	HBA port a	10
-	HBA port b	-	10
HBA port c	11	-	HBA port d

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:

MetroCluster eight-node configuration			
FibreBridge 7500 bridge	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	12	-
	FC2	-	12
bridge_x_1b	FC1	13	-
	FC2	-	13
bridge_x_2a	FC1	14	-
	FC2	-	14
bridge_x_2b	FC1	15	-
	FC2	-	15
bridge_x_3a	FC1	16	-
	FC2	-	16

MetroCluster eight-node configuration			
bridge_x_3b	FC1	17	-
	FC2	-	17
bridge_x_4a	FC1	18	-
	FC2	-	18
bridge_x_4b	FC1	19	-
	FC2	-	19

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

MetroCluster eight-node configuration			
FibreBridge 6500 bridge	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	12	-
bridge_x_1b	FC1	-	12
bridge_x_2a	FC1	13	-
bridge_x_2b	FC1	-	13
bridge_x_3a	FC1	14	-
bridge_x_3b	FC1	-	14
bridge_x_4a	FC1	15	-
bridge_x_4b	FC1	-	15
bridge_x_5a	FC1	16	-
bridge_x_5b	FC1	-	16
bridge_x_6a	FC1	17	-
bridge_x_6b	FC1	-	17
bridge_x_7a	FC1	18	-

MetroCluster eight-node configuration			
bridge_x_7b	FC1	-	18
bridge_x_8a	FC1	19	-
bridge_x_8b	FC1	-	19

Brocade port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster eight-node configuration		
ISL port	Brocade 6505, 6510, or DCX 8510-8	
	FC_switch_x_1	FC_switch_x_2
ISL port 1	20	20
ISL port 2	21	21
ISL port 3	22	22
ISL port 4	23	23

Brocade port usage for controllers in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

MetroCluster four-node configuration			
Component	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

MetroCluster four-node configuration			
controller_x_2	FC-VI port a	3	-
	FC-VI port b	-	3
	HBA port a	4	-
	HBA port b	-	4
	HBA port c	5	-
	HBA port d	-	5

Brocade port usage for bridges in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges. Additional bridges can be cabled to ports 18 through 23.

MetroCluster four-node configuration					
FibreBridge 7500 bridge	Port	Brocade 6510 or DCX 8510-8		Brocade 6505	
		FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	6	-	6	-
	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
	FC2	-	10	-	14

MetroCluster four-node configuration					
bridge_x_3b	FC1	11	-	15	-
	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
	FC2	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

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

FibreBridge 6500 bridge	Port	Brocade 6510, DCX 8510-8		Brocade 6505	
FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2		
bridge_x_1a	FC1	6	-	6	-
bridge_x_1b	FC1	-	6	-	6
bridge_x_2a	FC1	7	-	7	-
bridge_x_2b	FC1	-	7	-	7
bridge_x_3a	FC1	8	-	12	-
bridge_x_3b	FC1	-	8	-	12
bridge_x_4a	FC1	9	-	13	-
bridge_x_4b	FC1	-	9	-	13
bridge_x_5a	FC1	10	-	14	-
bridge_x_5b	FC1	-	10	-	14
bridge_x_6a	FC1	11	-	15	-

FibreBridge 6500 bridge	Port	Brocade 6510, DCX 8510-8		Brocade 6505	
bridge_x_6b	FC1	-	11	-	15
bridge_x_7a	FC1	12	-	16	-
bridge_x_7b	FC1	-	12	-	16
bridge_x_8a	FC1	13	-	17	-
bridge_x_8b	FC1	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

Brocade port usage for ISLs in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster four-node configuration				
ISL port	Brocade 6510, DCX 8510-8		Brocade 6505	
	FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
ISL port 1	20	20	8	8
ISL port 2	21	21	9	9
ISL port 3	22	22	10	10
ISL port 4	23	23	11	11

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.

MetroCluster two-node configuration			
Component	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2

MetroCluster two-node configuration			
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

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.

MetroCluster two-node configuration					
FibreBridge 7500 bridge	Port	Brocade 6510, DCX 8510-8		Brocade 6505	
		FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	6	-	6	-
	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
	FC2	-	10	-	14

MetroCluster two-node configuration					
bridge_x_3b	FC1	11	-	15	-
	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
	FC2	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

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

MetroCluster two-node configuration					
FibreBridge 6500 bridge	Port	Brocade 6510, DCX 8510-8 2z=		Brocade 6505	FC_switch_x_1
		FC_switch_x_2	FC_switch_x_1	FC_switch_x_2	bridge_x_1a
FC1	6	-	6	-	bridge_x_1b
FC1	-	6	-	6	bridge_x_2a
FC1	7	-	7	-	bridge_x_2b
FC1	-	7	-	7	bridge_x_3a
FC1	8	-	12	-	bridge_x_3b
FC1	-	8	-	12	bridge_x_4a
FC1	9	-	13	-	bridge_x_4b
FC1	-	9	-	13	bridge_x_5a
FC1	10	-	14	-	bridge_x_5b
FC1	-	10	-	14	bridge_x_6a

MetroCluster two-node configuration					
FC1	11	-	15	-	bridge_x_6b
FC1	-	11	-	15	bridge_x_7a
FC1	12	-	16	-	bridge_x_7b
FC1	-	12	-	16	bridge_x_8a
FC1	13	-	17	-	bridge_x_8b
FC1	-	13	-	17	

Brocade port usage for ISLs in a two-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster two-node configuration				
ISL port	Brocade 6510, DCX 8510-8		Brocade 6505	
	FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
ISL port 1	20	20	8	8
ISL port 2	21	21	9	9
ISL port 3	22	22	10	10
ISL port 4	23	23	11	11

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			
Component	Port	Cisco 9148 or 9148S	
		FC_switch_x_1	FC_switch_x_2

MetroCluster eight-node configuration			
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3
controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6
controller_x_3	FC-VI port a	7	
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9

MetroCluster eight-node configuration			
controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

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			
FibreBridge 7500 bridge	Port	Cisco 9148 or 9148S	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	14	14
	FC2	-	-
bridge_x_1b	FC1	15	15
	FC2	-	-
bridge_x_2a	FC1	17	17
	FC2	-	-
bridge_x_2b	FC1	18	18
	FC2	-	-
bridge_x_3a	FC1	19	19
	FC2	-	-

MetroCluster eight-node configuration			
bridge_x_3b	FC1	21	21
	FC2	-	-
bridge_x_4a	FC1	22	22
	FC2	-	-
bridge_x_4b	FC1	23	23
	FC2	-	-
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.

FibreBridge 6500 bridge	Port	Cisco 9148 or 9148S	
FC_switch_x_1	FC_switch_x_2		
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21

FibreBridge 6500 bridge	Port	Cisco 9148 or 9148S	
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23
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:

MetroCluster eight-node configuration		
.2+ ISL port	Cisco 9148 or 9148S	
FC_switch_x_1	FC_switch_x_2	ISL port 1
12	12	ISL port 2
16	16	ISL port 3
20	20	ISL port 4

Cisco port usage for controllers in a four-node MetroCluster configuration

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco switches:

MetroCluster four-node configuration			
Component	Port	Cisco 9148, 9148S, or 9250i	
		FC_switch_x_1	FC_switch_x_2

MetroCluster four-node configuration			
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3
controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6

Cisco port usage for FC-to-SAS bridges in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges. Additional bridges can be attached to ports 15 through 32 following the same pattern.

MetroCluster four-node configuration			
FibreBridge 7500 bridge	Port	Cisco 9148, 9148S, or 9250i	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
	FC2	-	7
bridge_x_1b	FC1	8	-
	FC2	-	8

MetroCluster four-node configuration			
bridge_x_2a	FC1	9	-
	FC2	-	9
bridge_x_2b	FC1	10	-
	FC2	-	10
bridge_x_3a	FC1	11	-
	FC2	-	11
bridge_x_3b	FC1	12	-
	FC2	-	12
bridge_x_4a	FC1	13	-
	FC2	-	13
bridge_x_4b	FC1	14	-
	FC2	-	14

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.

FibreBridge 6500 bridge	Port	Cisco 9148, 9148S, or 9250i	
FC_switch_x_1	FC_switch_x_2		
bridge_x_1a	FC1	7	-
bridge_x_1b	FC1	-	7
bridge_x_2a	FC1	8	-
bridge_x_2b	FC1	-	8
bridge_x_3a	FC1	9	-
bridge_x_3b	FC1	-	9
bridge_x_4a	FC1	10	-

FibreBridge 6500 bridge	Port	Cisco 9148, 9148S, or 9250i	
bridge_x_4b	FC1	-	10
bridge_x_5a	FC1	11	-
bridge_x_5b	FC1	-	11
bridge_x_6a	FC1	12	-
bridge_x_6b	FC1	-	12
bridge_x_7a	FC1	13	-
bridge_x_7b	FC1	-	13
bridge_x_8a	FC1	14	-
bridge_x_8b	FC1	-	14
Additional bridges can be attached to ports 15 through 32 following the same pattern.			

Cisco 9148 and 9148S port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage:

MetroCluster four-node configuration		
ISL port	Cisco 9148 or 9148S	
	FC_switch_x_1	FC_switch_x_2
ISL port 1	36	36
ISL port 2	40	40
ISL port 3	44	44
ISL port 4	48	48

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.

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			
Component	Port	Cisco 9148, 9148S, or 9250i	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3

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.

MetroCluster two-node configuration			
FibreBridge 7500 bridge	Port	Cisco 9148, 9148S, or 9250i	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
	FC2	-	7
bridge_x_1b	FC1	8	-
	FC2	-	8
bridge_x_2a	FC1	9	-
	FC2	-	9
bridge_x_2b	FC1	10	-
	FC2	-	10

MetroCluster two-node configuration			
bridge_x_3a	FC1	11	-
	FC2	-	11
bridge_x_3b	FC1	12	-
	FC2	-	12
bridge_x_4a	FC1	13	-
	FC2	-	13
bridge_x_4b	FC1	14	-
	FC2	-	14

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			
FibreBridge 6500 bridge	Port	Cisco 9148, 9148S, or 9250i	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1b	FC1	-	7
bridge_x_2a	FC1	8	-
bridge_x_2b	FC1	-	8
bridge_x_3a	FC1	9	-
bridge_x_3b	FC1	-	9
bridge_x_4a	FC1	10	-
bridge_x_4b	FC1	-	10
bridge_x_5a	FC1	11	-
bridge_x_5b	FC1	-	11

MetroCluster two-node configuration			
bridge_x_6a	FC1	12	-
bridge_x_6b	FC1	-	12
bridge_x_7a	FC1	13	-
bridge_x_7b	FC1	-	13
bridge_x_8a	FC1	14	-
bridge_x_8b	FC1	-	14
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:

MetroCluster two-node configuration		
ISL port	Cisco 9148 or 9148S	
	FC_switch_x_1	FC_switch_x_2
ISL port 1	36	36
ISL port 2	40	40
ISL port 3	44	44
ISL port 4	48	48

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.

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 or later

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 except for the Cisco 9250i switch.

  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.
- AFF A400 and FAS8300 storage systems use ports 2a and 2b for FC-VI connectivity.
- 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, G630, G620-1, G630-1, and G720 switches.

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.

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

Component	Port	Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 and DCX 8510-8		Brocade switch model G720
		Connects to FC switch…	Connects to switch port…	Connects to switch port…
Stack 1	bridge_x_1a	1	8	10
	bridge_x_1b	2	8	10
Stack 2	bridge_x_2a	1	9	11
	bridge_x_2b	2	9	11
Stack 3	bridge_x_3a	1	10	14
	bridge_x_4b	2	10	14
Stack y	bridge_x_ya	1	11	15
	bridge_x_yb	2	11	15

- On G620, G630, G620-1 and G630-1 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.
- On G720 switches, additional bridges can be cabled to ports 16 - 17, 20 and 21.

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

MetroCluster 2 or DR Group 2

			Brocade switch model				
Component	Port	Connects to FC_switch …	6510, DCX 8510-8	6520	7840, DCX 8510-8	G620, G620-1, G630, G630-1	G720

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only							
controller_x_3	FC-VI port a	1	24	48	12	18	18
	FC-VI port b	2	24	48	12	18	18
	FC-VI port c	1	25	49	13	19	19
	FC-VI port d	2	25	49	13	19	19
	HBA port a	1	26	50	14	24	26
	HBA port b	2	26	50	14	24	26
	HBA port c	1	27	51	15	25	27
	HBA port d	2	27	51	15	25	27
controller_x_4	FC-VI port a	1	28	52	16	22	22
	FC-VI port b	2	28	52	16	22	22
	FC-VI port c	1	29	53	17	23	23
	FC-VI port d	2	29	53	17	23	23
	HBA port a	1	30	54	18	28	30
	HBA port b	2	30	54	18	28	30
	HBA port c	1	31	55	19	29	31
	HBA port d	2	32	55	19	29	31
Stack 1	bridge_x_51a	1	32	56	20	26	32
	bridge_x_51b	2	32	56	20	26	32
Stack 2	bridge_x_52a	1	33	57	21	27	33
	bridge_x_52b	2	33	57	21	27	33

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only							
Stack 3	bridge_x_53a	1	34	58	22	30	34
	bridge_x_54b	2	34	58	22	30	34
Stack y .2a	bridge_x_ya	1	35	59	23	31	35
	bridge_x_yb	2	35	59	23	31	35

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)					
MetroCluster 1 or DR Group 1					
Component		Port	Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1, and DCX 8510-8		Brocade switch G720
			Connects to FC_switch…	Connects to switch port…	Connects to switch port…
Stack 1	bridge_x_1a	FC1	1	8	10
		FC2	2	8	10
	bridge_x_1B	FC1	1	9	11
		FC2	2	9	11
Stack 2	bridge_x_2a	FC1	1	10	14
		FC2	2	10	14
	bridge_x_2B	FC1	1	11	15
		FC2	2	11	15
Stack 3	bridge_x_3a	FC1	1	12*	16
		FC2	2	12*	16
	bridge_x_3B	FC1	1	13*	17
		FC2	2	13*	17

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)					
Stack y	bridge_x_ya	FC1	1	14*	20
		FC2	2	14*	20
	bridge_x_yb	FC1	1	15*	21
		FC2	2	15*	21

- - Ports 12 through 15 are reserved for the second MetroCluster or DR group on the Brocade 7840 switch.

Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620, G630, G620-1 and G630-1 switches.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)							
MetroCluster 2 or DR Group 2							
Component	Port	Brocade switch model					
		Connects to FC_switch …	6510, DCX 8510-8	6520	7840, DCX 8510-8	G620, G620-1, G630, G630-1	G720
controller_x_3	FC-VI port a	1	24	48	12	18	18
	FC-VI port b	2	24	48	12	18	18
	FC-VI port c	1	25	49	13	19	19
	FC-VI port d	2	25	49	13	19	19
	HBA port a	1	26	50	14	24	26
	HBA port b	2	26	50	14	24	26
	HBA port c	1	27	51	15	25	27
	HBA port d	2	27	51	15	25	27

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)								
controller_x_4		FC-VI port a	1	28	52	16	22	22
		FC-VI port b	2	28	52	16	22	22
		FC-VI port c	1	29	53	17	23	23
		FC-VI port d	2	29	53	17	23	23
		HBA port a	1	30	54	18	28	30
		HBA port b	2	30	54	18	28	30
		HBA port c	1	31	55	19	29	31
		HBA port d	2	31	55	19	29	31
Stack 1	bridge_x_51a	FC1	1	32	56	20	26	32
		FC2	2	32	56	20	26	32
	bridge_x_51b	FC1	1	33	57	21	27	33
		FC2	2	33	57	21	27	33
Stack 2	bridge_x_52a	FC1	1	34	58	22	30	34
		FC2	2	34	58	22	30	34
	bridge_x_52b	FC1	1	35	59	23	31	35
		FC2	2	35	59	23	31	35

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)								
Stack 3	bridge_x_53a	FC1	1	36	60	-	32	36
		FC2	2	36	60	-	32	36
	bridge_x_53b	FC1	1	37	61	-	33	37
		FC2	2	37	61	-	33	37
Stack y	bridge_x_5ya	FC1	1	38	62	-	34	38
		FC2	2	38	62	-	34	38
	bridge_x_5yb	FC1	1	39	63	-	35	39
		FC2	2	39	63	-	35	39
Additional bridges can be cabled to ports 36 to 39 in G620, G630, G620-1, and G630-1 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.

AFF A700 or FAS9000 systems support up to eight ISLs for improved performance. Eight ISLs are supported on the Brocade 6510 and G620 switches.

Switch model	ISL port	Switch port
Brocade 6520	ISL port 1	23
	ISL port 2	47
	ISL port 3	71
	ISL port 4	95
Brocade 6505	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Switch model	ISL port	Switch port
Brocade 6510 and Brocade DCX 8510-8	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47
Brocade 7810	ISL port 1	ge2 (10-Gbps)
	ISL port 2	ge3(10-Gbps)
	ISL port 3	ge4 (10-Gbps)
	ISL port 4	ge5 (10-Gbps)
	ISL port 5	ge6 (10-Gbps)
	ISL port 6	ge7 (10-Gbps)
Brocade 7840  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.	ISL port 1	ge0 (40-Gbps) or ge2 (10-Gbps)
	ISL port 2	ge1 (40-Gbps) or ge3 (10-Gbps)
	ISL port 3	ge10 (10-Gbps)
	ISL port 4	ge11 (10-Gbps)

Switch model	ISL port	Switch port
Brocade G610	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23
Brocade G620, G620-1, G630, G630-1, G720	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47

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.

Cisco 9396S			
Component	Port	Switch 1	Switch 2

Cisco 9396S			
controller_x_3	FC-VI port a	49	
	FC-VI port b	-	49
	FC-VI port c	50	
	FC-VI port d	-	50
	HBA port a	51	
	HBA port b	-	51
	HBA port c	52	
	HBA port d	-	52
controller_x_4	FC-VI port a	53	-
	FC-VI port b	-	53
	FC-VI port c	54	-
	FC-VI port d	-	54
	HBA port a	55	-
	HBA port b	-	55
	HBA port c	56	-
	HBA port d	-	56

Cisco 9148S			
Component	Port	Switch 1	Switch 2

Cisco 9148S			
controller_x_3	FC-VI port a	25	
	FC-VI port b	-	25
	FC-VI port c	26	-
	FC-VI port d	-	26
	HBA port a	27	-
	HBA port b	-	27
	HBA port c	28	-
	HBA port d	-	28
controller_x_4	FC-VI port a	29	-
	FC-VI port b	-	29
	FC-VI port c	30	-
	FC-VI port d	-	30
	HBA port a	31	-
	HBA port b	-	31
	HBA port c	32	-
	HBA port d	-	32

Cisco 9132T			
MDS module 1			
Component	Port	Switch 1	Switch 2
MDS module 2			
Component	Port	Switch 1	Switch 2

Cisco 9132T			
controller_x_3	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4
controller_x_4	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8

The following table shows systems with two FC-VI ports. AFF A700 and FAS9000 systems have four FC-VI ports (a, b, c, and d). If using an AFF A700 or FAS9000 system, the port assignments move along by one position. For example, FC-VI ports c and d go to switch port 2 and HBA ports a and b go to switch port 3.

Cisco 9250i*			
Component	Port	Switch 1	Switch 2

Cisco 9250i*			
controller_x_3	FC-VI port a	7	-
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9
controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

- - 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

Cisco 9396S			
FibreBridge 7500 using two FC ports	Port	Switch 1	Switch 2
bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11

Cisco 9396S			
bridge_x_2b	FC1	12	-
	FC2	-	12
bridge_x_3a	FC1	13	-
	FC2	-	13
bridge_x_3b	FC1	14	-
	FC2	-	14
bridge_x_4a	FC1	15	-
	FC2	-	15
bridge_x_4b	FC1	16	-
	FC2	-	16
		Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.	

Cisco 9148S			
FibreBridge 7500 using two FC ports	Port		
		Switch 1	Switch 2
bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12

Cisco 9148S			
bridge_x_3a	FC1	13	-
	FC2	-	13
bridge_x_3b	FC1	14	-
	FC2	-	14
bridge_x_4a	FC1	15	-
	FC2	-	15
bridge_x_4b	FC1	16	-
	FC2	-	16

Cisco 9132T			
FibreBridge 7500 using two FC ports	Port		
		Switch 1	Switch 2
bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12
		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 9250i			
FibreBridge 7500 using two FC ports	Port		
		Switch 1	Switch 2
bridge_x_1a	FC1	14	-
	FC2	-	14
bridge_x_1b	FC1	15	-
	FC2	-	15
bridge_x_2a	FC1	17	-
	FC2	-	17
bridge_x_2b	FC1	18	-
	FC2	-	18
bridge_x_3a	FC1	19	-
	FC2	-	19
bridge_x_3b	FC1	21	-
	FC2	-	21
bridge_x_4a	FC1	22	-
	FC2	-	22
bridge_x_4b	FC1	23	-
	FC2	-	23
		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.

FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	Port	Cisco 9396S	
Switch 1	Switch 2		
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16
		Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.	

FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	Port	Cisco 9148S	
Switch 1	Switch 2		
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16
		Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.	

Cisco 9250i			
FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	Port	Switch 1	Switch 2

Cisco 9250i			
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23
		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.

Switch model	ISL port	Switch port
Cisco 9396S	ISL 1	44
	ISL 2	48
	ISL 3	92
	ISL 4	96
Cisco 9250i with 24 port license	ISL 1	12
	ISL 2	16
	ISL 3	20
	ISL 4	24
Cisco 9148S	ISL 1	20
	ISL 2	24
	ISL 3	44
	ISL 4	48
Cisco 9132T	ISL 1	MDS module 1 port 13
	ISL 2	MDS module 1 port 14
	ISL 3	MDS module 1 port 15
	ISL 4	MDS module 1 port 16

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.

This task is not required on two-node MetroCluster configurations.

This task must be performed at both MetroCluster sites.

Steps

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.

AFF and FAS Documentation Center

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.

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.

Steps

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

   Cluster peering can be done on dedicated ports or on data ports. Using dedicated ports provides higher throughput for the cluster peering traffic.

   Cluster and SVM peering express configuration

Related information

Cluster and SVM peering express configuration

Considerations for configuring cluster peering

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.

- 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.

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.

Steps

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.

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.

Configuring the FC switches by running a configuration file

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

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.

Configuring Brocade FC switches with RCF files

To configure a Brocade FC switch, you must reset the switch settings to factory defaults, install the switch software, and download and apply the reference configuration (RCF) files that provide the complete switch settings for certain configurations.

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

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.

Resetting the Brocade FC switch to factory defaults

Before installing a new software version and RCF files, you must erase the current switch configuration and perform basic configuration.

You must repeat these steps on each of the FC switches in the MetroCluster fabric configuration.

1. Log in to the switch as an administrator.
2. Disable the Brocade Virtual Fabrics (VF) feature: **`fosconfig options`**

```
FC_switch_A_1:admin> fosconfig --disable vf
WARNING:  This is a disruptive operation that requires a reboot to take
effect.
Would you like to continue  [Y/N]: y
```

3. Disconnect the ISL cables from the ports on the switch.
4. Disable the switch: **`switchcfgpersistentdisable`**

```
FC_switch_A_1:admin> switchcfgpersistentdisable
```

5. Disable the configuration: **`cfgDisable`**

```
FC_switch_A_1:admin> cfgDisable
You are about to disable zoning configuration. This action will disable
any previous zoning configuration enabled.
Do you want to disable zoning configuration? (yes, y, no, n): [no] y
Updating flash ...
Effective configuration is empty. "No  Access" default zone mode is ON.
```

6. Clear the configuration: **`cfgClear`**

```
FC_switch_A_1:admin> cfgClear
The Clear All action will clear all Aliases, Zones, FA Zones
and configurations in the Defined configuration.
Run cfgSave to commit the transaction or cfgTransAbort to
cancel the transaction.
Do you really want to clear all configurations?  (yes, y, no, n): [no] y
```

7. Save the configuration: **`cfgSave`**

```
FC_switch_A_1: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] y
Updating flash ...
```

8. Set the default configuration: **configDefault**

```
FC_switch_A_1:admin> configDefault
WARNING:  This is a disruptive operation that requires a switch reboot.
Would you like to continue [Y/N]: y
Executing configdefault...Please wait
2020/10/05-08:04:08, [FCR-1069], 1016, FID 128, INFO, FC_switch_A_1, The
FC Routing service is enabled.
2020/10/05-08:04:08, [FCR-1068], 1017, FID 128, INFO, FC_switch_A_1, The
FC Routing service is disabled.
2020/10/05-08:04:08, [FCR-1070], 1018, FID 128, INFO, FC_switch_A_1, The
FC Routing configuration is set to default.
Committing configuration ... done.
2020/10/05-08:04:12, [MAPS-1113], 1019, FID 128, INFO, FC_switch_A_1,
Policy dflt_conservative_policy activated.
2020/10/05-08:04:12, [MAPS-1145], 1020, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for E-Ports.
2020/10/05-08:04:12, [MAPS-1144], 1021, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for F-Ports.
The switch has to be rebooted to allow the changes to take effect.
2020/10/05-08:04:12, [CONF-1031], 1022, FID 128, INFO, FC_switch_A_1,
configDefault completed successfully for switch.
```

9. Set the port configuration to default for all ports:

   portcfgdefault *port-number*

```
FC_switch_A_1:admin> portcfgdefault <port number>
```

   You must complete this step for each port.

10. Verify that the switch is using the dynamic Port on Demand (POD) method.

> For Brocade Fabric OS versions before 8.0, you run the following commands as admin, and for versions 8.0 and later, you run them as root.

   a. Run the command **licenseport --show**

```
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
```

b. Enable the root user if it is disabled by Brocade.

```
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**

```
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**

If the dynamic POD method is not in use (if POD method is in static) you must change the license assignment method to dynamic. Skip this step if the dynamic POD method is in use.

```
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
```

11. Reboot the switch: **fastBoot**

```
FC_switch_A_1:admin> fastboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
```

12. Confirm that the default settings have been implemented: **switchShow**
13. Verify that the IP address is set correctly: **ipAddrShow**

    You can set the IP address with the following command, if required: **ipAddrSet**

Downloading the Brocade FC switch RCF file

You must download the reference configuration (RCF) file to each switch in the MetroCluster fabric configuration.

To use these RCF files, the system must be running ONTAP 9.1 or later and you must use the port layout for ONTAP 9.1 or later.

If you are planning to use only one of the FC ports on the FibreBridge bridges, configure the back-end fibre channel switches manually using the instructions found in the section, Port assignments for FC switches when using ONTAP 9.1 and later.

Steps

1. Refer to the RCF file table on the Brocade RCF download page and identify the correct RCF file for each switch in your configuration.

   The RCF files must be applied to the correct switches.

2. Download the RCF files for the switches from the Brocade RCF download page.

   The files must be placed in a location where they can be transferred to the switch. There is a separate file for each of the four switches that make up the two-switch fabric.

3. Repeat these steps on each switch in the configuration.

Installing the Brocade FC switch RCF file

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

These steps must be repeated on each of the Brocade FC switches in the MetroCluster fabric configuration.

Steps

1. Initiate the download and configuration process:

   configDownload

   Respond to the prompts as shown in the following example.

```
FC_switch_A_1:admin> configDownload
Protocol (scp, ftp, sftp, local) [ftp]:
Server Name or IP Address [host]: <user input>
User Name [user]:<user input>
Path/Filename [<home dir>/config.txt]:path to configuration file
Section (all|chassis|switch [all]): all
.
.
.
Do you want to continue [y/n]: y
Password: <user input>
```

After entering your password, the switch downloads and executes the configuration file.

2. Persistently enable the switch: **switchcfgpersistentenable**

   The example shows how to persistently enable FC switch_A_1.

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

3. Run the following command to confirm that the configuration file has set the switch domain:

   switchShow

   Each switch is assigned a different domain number depending on which configuration file the switch used.

```
FC_switch_A_1:admin> switchShow
switchName: FC_switch_A_1
switchType: 109.1
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 5
```

4. Verify that your switch is assigned the correct domain value as indicated in the following table.

Fabric	Switch	Switch domain
1	A_1	5
	B_1	7
2	A_2	6
	B_2	8

5. Change the port speed: **portcfgspeed**

```
FC_switch_A_1:admin> portcfgspeed port number port speed
```

By default, all the ports are configured to operate at 16 Gbps. You might change the port speed for the following reasons:

- The interconnect switch ports speed should be changed when an 8-Gbps FC-VI adapter is used and the switch port speed should set to 8 Gbps.
- The switch ports speed should be changed when an 8-Gbps HBA adapter is used for ATTO FibreBridge 6500N.

- The ISL ports' speed must be changed when the ISL is not capable of running at 16 Gbps. ====

1. Calculate the ISL distance.

   Due to the behavior of the FC-VI, you must set the distance to 1.5 times the real distance with a minimum of 10 (LE). The distance for the ISL is calculated as follows, rounded up to the next full kilometer: 1.5 × real distance = distance.

   If the distance is 3 km, then 1.5 × 3 km = 4.5. This is lower than 10; therefore, you must set the ISL to the LE distance level.

   The distance is 20 km, then 1.5 × 20 km = 30. You must set the ISL to the LS distance level.

2. Set the distance for each ISL port using the following command: **portcfglongdistance** *port levelvc_link_initdistance*

   A vc_link_init value of 1 uses the fillword 'ARB' by default. A value of 0 uses the fillword 'IDLE'. The required value might vary depending on the link you use. In this example, the default is set and the distance is assumed to be 20 km. Hence, the setting is '30' with a vc_link_init value of 1, and the ISL port is 21.

   Example: LS

   ```
   FC_switch_A_1:admin> portcfglongdistance 21 LS 1
   -distance 30
   ```

   Example: LE

   ```
   FC_switch_A_1:admin> portcfglongdistance 21 LE 1
   ```

3. Verify if the IP address is set correctly: **ipAddrshow**

   ```
   FC_switch_A_1:admin> ipAddrshow
   ```

   You can set the IP address with the following command if required: **ipAddrSet**

4. Set the timezone from the switch prompt: **tstimezone --interactive**

   You should respond to the prompts as required.

   ```
   FC_switch_A_1:admin>  tstimezone --interactive
   ```

5. Reboot the switch: **reboot**

   The example shows how to reboot FC switch _A_1.

```
FC_switch_A_1:admin> reboot
```

6. Verify the distance setting: **portbuffershow**

   A distance setting of LE appears as 10 km.

```
FC_Switch_A_1:admin> portbuffershow
User Port Lx   Max/Resv Buffer Needed  Link
Remaining
Port Type Mode Buffers  Usage  Buffers Distance
Buffers
---- ---- ---- ------- ------ ------- ---------
----------
...
21    E    -      8      67     67      30 km
22    E    -      8      67     67      30 km
...
23    -    8      0       -      -      466
```

7. Reconnect the ISL cables to the ports on the switches where they were removed.

   The ISL cables were disconnected when the factory settings were reset to the default settings.

   Resetting the Brocade FC switch to factory defaults

8. Validate the configuration.

   a. Verify that the switches form one fabric: **switchshow**

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

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
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)
...
```

b. Confirm the configuration of the fabrics: **fabricshow**

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC
IP Addr Name
-------------------------------------------------
--------------
1: fffc01 10:00:00:05:33:86:89:cb 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"
```

c. Very that the ISLs are working: **islshow**

```
FC_switch_A_1:admin> islshow
```

d. Confirm that zoning is properly replicated by running the following commands:
cfgshow
zoneshow

Both outputs should show the same configuration information and zoning

information for both switches.

e. If trunking is used, you can confirm the trunking with the following command:
trunkShow

```
FC_switch_A_1:admin> trunkshow
```

= Configuring the Cisco FC switches with RCF files :icons: font

To configure a Cisco FC switch, you must reset the switch settings to factory defaults, install the switch software, and download and apply the reference configuration (RCF) files that provide the complete switch settings for certain configurations.

= Resetting the Cisco FC switch to factory defaults :icons: font

Before installing a new software version and RCFs, you must erase the Cisco switch configuration and perform basic configuration.

You must repeat these steps on each of the FC switches in the MetroCluster fabric configuration.

The outputs shown are for Cisco IP switches; however, these steps are also applicable for Cisco FC switches.

Steps

1. Reset the switch to factory defaults:
   a. Erase the existing configuration:
   write erase
   b. Reload the switch software:
   reload

   The system reboots and enters the configuration wizard. During the boot, if you receive the prompt Abort Auto Provisioning and continue with normal setup?(yes/no)[n], you should respond **yes** to proceed.

   c. In the configuration wizard, enter the basic switch settings:
      - Admin password
      - Switch name
      - Out-of-band management configuration
      - Default gateway
      - SSH service (Remote Support Agent) After completing the configuration wizard, the switch reboots.
   d. When prompted, enter the user name and password to log in to the switch.

   The following example shows the prompts and system responses when logging

in to the switch. The angle brackets (<<<) show where you enter the information.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard
(yes/no) [y]:y  **<<<**

    Enter the password for "admin": password  **<<<**
  Confirm the password for "admin": password  **<<<**
         ---- Basic System Configuration Dialog VDC:
1 ----

This setup utility will guide you through the basic
configuration of
the system. Setup configures only enough connectivity
for management
of the system.

Please register Cisco Nexus3000 Family devices
promptly with your
supplier. Failure to register may affect response
times for initial
service calls. Nexus3000 devices must be registered
to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c
at anytime
to skip the remaining dialogs.
```

e. Enter basic information in the next set of prompts, including the switch name, management address, and gateway, and enter **rsa** for the SSH key as shown in the example:

```
Would you like to enter the basic configuration
dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no)
[n]:
  Configure read-write SNMP community string (yes/no)
[n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management
configuration? (yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address
**<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask
**<<<**
  Configure the default gateway? (yes/no) [y]: y
**<<<**
    IPv4 address of the default gateway : gateway-IP-
address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate
(dsa/rsa) [rsa]: rsa **<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state
(shut/noshut) [noshut]: shut **<<<**
  Configure CoPP system profile
(strict/moderate/lenient/dense) [strict]:
```

The final set of prompt completes the configuration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no)
[n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-
COPP_POLICY: Control-Plane is protected with policy
copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Save the configuration:

```
IP_switch_A_1# copy running-config startup-config
```

3. Reboot the switch and wait for the switch to reload:

```
IP_switch_A_1# reload
```

4. Repeat the previous steps on the other three switches in the MetroCluster fabric configuration.

= Downloading and installing the Cisco FC switch NX-OS software :icons: font

You must download the switch operating system file and RCF file to each switch in the MetroCluster fabric configuration.

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

These steps must be repeated on each of the FC switches in the MetroCluster fabric configuration.

You must use the supported switch software version.

NetApp Hardware Universe

The outputs shown are for Cisco IP switches; however, these steps are also applicable for Cisco FC switches.

1. Download the supported NX-OS software file.

   Cisco download page

2. Copy the switch software to the switch:

   +copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management+

   In this example, the `nxos.7.0.3.I4.6.bin` file is copied from SFTP server 10.10.99.99 to the local bootflash:

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to
/bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                  100%
666MB   7.2MB/s   01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
```

3. Verify on each switch that the switch NX-OS files are present in each switch's bootflash directory:

dir bootflash

The following example shows that the files are present on `IP_switch_A_1`:

```
IP_switch_A_1# dir bootflash:
                    .
                    .
                    .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                    .
                    .
                    .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Install the switch software:

install all system bootflash:nxos.version-number.bin kickstart bootflash:nxos.version-kickstart-number.bin

```
IP_switch_A_1#  install all system
bootflash:nxos.7.0.3.I4.6.bin kickstart
bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please
wait.

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot
variable "kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot
variable "system".
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "system" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS
...
```

The switch reboot automatically after the switch software has installed.

5. Wait for the switch to reload and then log in to the switch.

   After the switch has rebooted the login prompt is displayed:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verify that the switch software has been installed:

   show version

   The following example shows the output:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software
version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017
07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB
of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49
second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52
2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Repeat these steps on the remaining three FC switches in the MetroCluster fabric configuration.

= Downloading and installing the Cisco FC RCF files :icons: font

You must download the RCF file to each switch in the MetroCluster fabric configuration.

This task requires file transfer software, such as FTP, Trivial File Transfer Protocol (TFTP), SFTP, or Secure Copy Protocol (SCP), to copy the files to the switches.

These steps must be repeated on each of the Cisco FC switches in the MetroCluster fabric configuration.

You must use the supported switch software version.

NetApp Hardware Universe

There are four RCF files, one for each of the four switches in the MetroCluster fabric configuration. You must use the correct RCF files for the switch model you are using.

Switch	RCF file
FC_switch_A_1	`NX3232_v1.80_Switch-A1.txt`
FC_switch_A_2	`NX3232_v1.80_Switch-A2.txt`
FC_switch_B_1	`NX3232_v1.80_Switch-B1.txt`
FC_switch_B_2	`NX3232_v1.80_Switch-B2.txt`

The outputs shown are for Cisco IP switches; however, these steps are also applicable for Cisco FC switches.

Steps

1. Download the Cisco FC RCF files.
2. Copy the RCF files to the switches.
   a. Copy the RCF files to the first switch:
   copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF bootflash: vrf management

   In this example, the `NX3232_v1.80_Switch-A1.txt` RCF file is copied from the SFTP server at `10.10.99.99` to the local bootflash. You must use the IP address of your TFTP/SFTP server and the file name of the RCF file that you need to install.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.8T-
X1_Switch-A1.txt bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100%
5141     5.0KB/s   00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

b. Repeat the previous substep for each of the other three switches, being sure to copy the matching RCF file to the corresponding switch.

3. Verify on each switch that the RCF file is present in each switch's `bootflash` directory:

   `dir bootflash:`

   The following example shows that the files are present on IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
       5514    Jun 13 22:09:05 2017
NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Copy the matching RCF file from the local bootflash to the running configuration on each switch:

   `copy bootflash:`*`switch-specific-RCF`*`.txt running-config`

5. Copy the RCF files from the running configuration to the startup configuration on each switch:

   copy running-config startup-config

   You should see output similar to the following:

   ```
   IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt
   running-config
   IP_switch_A_1# copy running-config startup-config
   ```

6. Reload the switch: **reload**

   ```
   IP_switch_A_1# reload
   ```

7. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

= Configuring the Cisco or Brocade FC switches manually :icons: font

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

= Configuring the Brocade FC switches :icons: font

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

- 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.

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.

◦ 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

◦ 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.

== 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.

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

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.

   The following example shows the command on BrocadeSwitchA:

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

   The following example shows the command on BrocadeSwitchB:

   ```
   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.

   The following example shows the command on BrocadeSwitchA:

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

   The following example shows the command on BrocadeSwitchB:

   ```
   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.

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: `cfgdisablecfgclearcfgsave`

   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`

   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`

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`

   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`

   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:> defzone --noaccess
   FC_switch_A_1:> cfgsave
   FC_switch_A_1:> 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_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> 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`

    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.

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

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.

```
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.

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

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

   - The following steps must be performed on each switch fabric to configure IOD of frames:
     i. Enable IOD: `iodset`
     ii. Set the Advanced Performance Tuning (APT) policy to 1: `aptpolicy 1`
     iii. Disable Dynamic Load Sharing (DLS): `dlsreset`
     iv. 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
```

v. Repeat these steps on the second switch fabric.

- The following steps must be performed on each switch fabric to configure OOD of frames:
  i. Enable OOD: `iodreset`
  ii. Set the Advanced Performance Tuning (APT) policy to 3: `aptpolicy 3`
  iii. Disable Dynamic Load Sharing (DLS): `dlsreset`
  iv. 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
```

v. 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.

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

4. Verify that the switch is using the dynamic port licensing method.

   a. Run the `licensePort --show` command.

   ```
   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
   ```

   Brocade FabricOS 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:

   ```
   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`

   ```
   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`

   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.

```
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.

On FC_switch_A_1:

+

```
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'
Trap Recipient's IP address : [0.0.0.0]
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:

+

```
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'
Trap Recipient's IP address : [0.0.0.0]
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>
```

1. Reboot the switch: `reboot`

   On FC_switch_A_1:

   ```
   FC_switch_A_1:admin> reboot
   ```

   On FC_switch_B_1:

   ```
   FC_switch_B_1:admin> reboot
   ```

2. Persistently enable the switch: `switchcfgpersistentenable`

   On FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

   On FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchcfgpersistentenable
   ```

== Configuring basic switch settings on a Brocade DCX 8510-8 switch

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

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_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

In the previous example, domain IDs 5 and 7 form fabric_1, and domain IDs 6 and 8 form fabric_2.

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:

- LOGICAL FABRIC 1: Switch1/Blade1 and Switch 2 Blade 1
- LOGICAL FABRIC 2: Switch1/Blade2 and Switch 2 Blade 2

1. Enter the command mode: `configure`
2. Proceed through the prompts:
   a. Set the domain ID for the switch.
   b. Keep selecting **Enter** until you get to RDP Polling Cycle, and then set the value to `0` to disable the polling.
   c. Select **Enter** until you return to the switch prompt.

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = `5


RDP Polling Cycle(hours)[0 = Disable Polling]:
(0..24) [1] 0
`
```

3. 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`

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

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 information

Requirements for using a Brocade DCX 8510-8 switch

== 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.

- 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).

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.

Switch model	ISL port	Switch port
Brocade 6520	ISL port 1	23
ISL port 2	47	ISL port 3
71	ISL port 4	95
Brocade 6505	ISL port 1	20
ISL port 2	21	ISL port 3
22	ISL port 4	23
Brocade 6510 and Brocade DCX 8510-8	ISL port 1	40
ISL port 2	41	ISL port 3
42	ISL port 4	43
ISL port 5	44	ISL port 6
45	ISL port 7	46
ISL port 8	47	Brocade 7810

ISL port 1	ge2 (10-Gbps)	ISL port 2
ge3(10-Gbps)	ISL port 3	ge4 (10-Gbps)
ISL port 4	ge5 (10-Gbps)	ISL port 5
ge6 (10-Gbps)	ISL port 6	ge7 (10-Gbps)
Brocade 7840**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.	ISL port 1	ge0 (40-Gbps) or ge2 (10-Gbps)
ISL port 2	ge1 (40-Gbps) or ge3 (10-Gbps)	ISL port 3
ge10 (10-Gbps)	ISL port 4	ge11 (10-Gbps)
Brocade G610	ISL port 1	20
ISL port 2	21	ISL port 3
22	ISL port 4	23
Brocade G620, G620-1, G630, G630-1, G720	ISL port 1	40
ISL port 2	41	ISL port 3
42	ISL port 4	43
ISL port 5	44	ISL port 6
45	ISL port 7	46

1. Configure the port speed: `portcfgspeed port-numberspeed`

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

   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 portcfgtrunk port-numberport-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 portcfgtrunkport-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`

   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`

   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:

```
Ports of Slot 0   12  13   14 15    16  17  18  19   20
21 22  23    24  25  26  27
-----------------+---+---+---+---+-----+---+---+---+----+
```

```
---+---+---+-----+---+---+---
Speed             AN  AN  AN  AN    AN  AN  8G  AN   AN
AN  16G  16G    AN  AN  AN  AN
Fill Word         0   0   0   0     0   0   3   0    0
0   3   3     3   0   0   0
AL_PA Offset 13   ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Trunk Port        ..  ..  ..  ..    ..  ..  ..  ..   ON
ON  ..  ..    ..  ..  ..  ..
Long Distance     ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
VC Link Init      ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Locked L_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Locked G_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Disabled E_Port   ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Locked E_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
ISL R_RDY Mode    ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
RSCN Suppressed   ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Persistent Disable..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
LOS TOV enable    ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
NPIV capability   ON  ON  ON  ON    ON  ON  ON  ON   ON
ON  ON  ON    ON  ON  ON  ON
NPIV PP Limit    126 126 126 126   126 126 126 126  126
126 126 126   126 126 126 126
QOS E_Port        AE  AE  AE  AE    AE  AE  AE  AE   AE
AE  AE  AE    AE  AE  AE  AE
Mirror Port       ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Rate Limit        ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Credit Recovery   ON  ON  ON  ON    ON  ON  ON  ON   ON
ON  ON  ON    ON  ON  ON  ON
Fport Buffers     ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
Port Auto Disable ..  ..  ..  ..    ..  ..  ..  ..   ..
..  ..  ..    ..  ..  ..  ..
CSCTL mode        ..  ..  ..  ..    ..  ..  ..  ..   ..
```

```
..  ..  ..    ..  ..  ..  ..

Fault Delay       0  0  0  0    0  0  0  0   0  0  0  0
0  0  0  0
```

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 × real_distance = distance

   If the distance is 3 km, then 1.5 × 3 km = 4.5 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 × 20 km = 30 km. The ISL must be set to 30 km and must use the LS distance level.

6. Set the distance on each ISL port: `portcfglongdistance`portdistance-levelvc_link_initdistance

   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.

   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: `portbuffershow`

   A distance level of LE appears as 10 km.

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

```
FC_switch_A_1:admin> portbuffershow

User  Port     Lx      Max/Resv    Buffer Needed    Link
Remaining
Port  Type    Mode     Buffers     Usage  Buffers
Distance  Buffers
----  ----    ----     -------     ------ -------
--------- ---------
...
 20     E      -          8         67      67
30km
 21     E      -          8         67      67
30km
...
 23            -          8          0      -        -
466
```

8. Verify that both switches form one fabric: `switchshow`

   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
switchType: 109.1
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
switchType: 109.1
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_A_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`

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP
Addr Name
-----------------------------------------------------
---------
1: fffc01 10:00:00:05:33:86:89:cb 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 10:00:00:05:33:86:89:cb 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
       1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15
      MASTER
          21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16
      ```

    - 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 through Step 10 for the second FC switch fabric.

Related information

Port assignments for FC switches when using ONTAP 9.1 and later

== 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.

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.

1. Create IP interface (ipif) addresses for the 10 Gbps ports on both switches in the fabric: `portcfg ipif FC_switch1_namefirst_port_name create FC_switch1_IP_address netmask netmask_number vlan 2 mtu auto`

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

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.71 netmask
   255.255.0.0 vlan 2 mtu auto
   portcfg ipif  ge3.dp0 create  10.10.21.71 netmask
   255.255.0.0 vlan 2 mtu auto
   ```

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

```
portcfg ipif  ge2.dp0 create  10.10.20.72 netmask
255.255.0.0 vlan 2 mtu auto
portcfg ipif  ge3.dp0 create  10.10.21.72 netmask
255.255.0.0 vlan 2 mtu auto
```

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

   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
-----------------------------------------------------
--------------------------
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
-----------------------------------------------------
---------------------------
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 first of the two FCIP tunnels using the ports on dp0: `portcfg fciptunnel`

   This command creates a tunnel with a single circuit.

   The following command creates the tunnel on switch FC_switch_A_1:

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

4. Verify that the FCIP tunnels were successfully created: `portshow fciptunnel all`

   The following example shows that the tunnels were created and the circuits are up:

```
FC_switch_B_1:root>

 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 for dp0.

   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
   ```

6. Verify that all circuits were successfully created: `portshow fcipcircuit all`

   The following command shows the circuits and their status:

```
FC_switch_A_1:root> portshow fcipcircuit all

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps
RxMBps ConnCnt CommRt Met/G
--------------------------------------------------
---------------------------
 24    0 ge2     Up      ---va---4    2d12m    0.02
0.03   3 10000/10000 0/-
 24    1 ge3     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 40 Gbps VE-ports on Brocade 7810 and 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.

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.
- FC_switch_B_1 is remote.

1. Create IP interface (ipif) addresses for the 40 Gbps ports on both switches in the fabric: `portcfg ipif FC_switch_namefirst_port_name create FC_switch_IP_address netmask netmask_number vlan 2 mtu auto`

   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
   ```

   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`

   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 fciptunnel`

   The following command creates the tunnel on FC_switch_A_1:

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

   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: `portshow fciptunnel all`

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

   ```
   FC_switch_A_1:root>

    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`

   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: `portshow fcipcircuit all`

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

```
FC_switch_A_1:root> portshow fcipcircuit all

 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.

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

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

   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.

```
FC_switch_A_1:admin> portcfgspeed 6 16

FC_switch_B_1:admin> portcfgspeed 6 16
```

1. Verify the settings: `portcfgshow`

```
FC_switch_A_1:admin> portcfgshow

FC_switch_B_1:admin> portcfgshow
```

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

```
Ports of Slot 0                   0   1   2   3   4
5   6   7   8
----------------------------------+---+---+---+--+
---+---+---+---+--
Speed                             16G 16G 16G 16G
16G 16G 16G 16G 16G
AL_PA Offset 13                   ..  ..  ..  ..
..  ..  ..  ..  ..
Trunk Port                        ..  ..  ..  ..
..  ..  ..  ..  ..
Long Distance                     ..  ..  ..  ..
..  ..  ..  ..  ..
VC Link Init                      ..  ..  ..  ..
..  ..  ..  ..  ..
Locked L_Port                     -   -   -   -   -
-   -   -   -
Locked G_Port                     ..  ..  ..  ..
..  ..  ..  ..  ..
Disabled E_Port                   ..  ..  ..  ..
..  ..  ..  ..  ..
Locked E_Port                     ..  ..  ..  ..
..  ..  ..  ..  ..
ISL R_RDY Mode                    ..  ..  ..  ..
..  ..  ..  .. ..
RSCN Suppressed                   ..  ..  ..  ..
..  ..  ..  .. ..
Persistent Disable                ..  ..  ..  ..
..  ..  ..  .. ..
```

```
LOS TOV enable                          ..  ..  ..  ..
..  ..  ..  .. ..
NPIV capability                         ON  ON  ON  ON
ON  ON  ON  ON  ON
NPIV PP Limit                           126 126 126 126
126 126 126 126 126
QOS Port                                AE  AE  AE  AE
AE  AE  AE  AE  ON
EX Port                                 ..  ..  ..  ..
..  ..  ..  ..  ..
Mirror Port                             ..  ..  ..  ..
..  ..  ..  ..  ..
Rate Limit                              ..  ..  ..  ..
..  ..  ..  ..  ..
Credit Recovery                         ON  ON  ON  ON
ON  ON  ON  ON  ON
Fport Buffers                           ..  ..  ..  ..
..  ..  ..  ..  ..
Eport Credits                           ..  ..  ..  ..
..  ..  ..  ..  ..
Port Auto Disable                       ..  ..  ..  ..
..  ..  ..  ..  ..
CSCTL mode                              ..  ..  ..  ..
..  ..  ..  ..  ..
D-Port mode                             ..  ..  ..  ..
..  ..  ..  ..  ..
D-Port over DWDM                        ..  ..  ..  ..
..  ..  ..  ..  ..
FEC                                     ON  ON  ON  ON
ON  ON  ON  ON  ON
Fault Delay                             0   0   0   0   0
0   0   0   0
Non-DFE                                 ..  ..  ..  ..
..  ..  ..  ..  ..
```

== Configuring compression on ISL ports on 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.

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

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.

```
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.

```
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.

```
FC_switch_A_1:admin> portenccompshow
User      Encryption                  Compression
Config
Port   Configured    Active   Configured   Active  Speed
----   ----------    -------  ----------   ------  -----
  0    Yes            Yes        Yes             Yes
16G
```

== 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.

=== 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.

DR group 1 : QOSH1 FC-VI zone for FC-VI port a / c

FC switch	Site	Switch domain	6505 / 6510 port	6520 port	G620 port	Connects to…
FC_switch _A_1	A	5	0	0	0	controller_ A_1 port FC-VI a
FC_switch _A_1	A	5	1	1	1	controller_ A_1 port FC-VI c
FC_switch _A_1	A	5	4	4	4	controller_ A_2 port FC-VI a
FC_switch _A_1	A	5	5	5	5	controller_ A_2 port FC-VI c
FC_switch _B_1	B	7	0	0	0	controller_ B_1 port FC-VI a
FC_switch _B_1	B	7	1	1	1	controller_ B_1 port FC-VI c
FC_switch _B_1	B	7	4	4	4	controller_ B_2 port FC-VI a
FC_switch _B_1	B	7	5	5	5	controller_ B_2 port FC-VI c

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

FC switch	Site	Switch domain	6505 / 6510 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	0	0	0	controller_A_1 port FC-VI b
			1	1	1	controller_A_1 port FC-VI d
			4	4	4	controller_A_2 port FC-VI b
			5	5	5	controller_A_2 port FC-VI d
FC_switch_B_2	B	8	0	0	0	controller_B_1 port FC-VI b
			1	1	1	controller_B_1 port FC-VI d
			4	4	4	controller_B_2 port FC-VI b
			5	5	5	controller_B_2 port FC-VI d

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

FC switch	Site	Switch domain	Switch port			Connects to…
			6510	6520	G620	
FC_switch_A_1	A	5	24	48	18	controller_A_3 port FC-VI a
			25	49	19	controller_A_3 port FC-VI c

FC switch	Site	Switch domain	Switch port			Connects to…
			28	52	22	controller_A_4 port FC-VI a
			29	53	23	controller_A_4 port FC-VI c
FC_switch_B_1	B	7	24	48	18	controller_B_3 port FC-VI a
			25	49	19	controller_B_3 port FC-VI c
			28	52	22	controller_B_4 port FC-VI a
			29	53	23	controller_B_4 port FC-VI c

Zone in Fabric_1	Member ports
QOSH2_MC2_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
QOSH2_MC2_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53

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

FC switch	Site	Switch domain	6510 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	24	48	18	controller_A_3 port FC-VI b
FC_switch_A_2	A	6	25	49	19	controller_A_3 port FC-VI d
FC_switch_A_2	A	6	28	52	22	controller_A_4 port FC-VI b
FC_switch_A_2	A	6	29	53	23	controller_A_4 port FC-VI d
FC_switch_B_2	B	8	24	48	18	controller_B_3 port FC-VI b

FC switch	Site	Switch domain	6510 port	6520 port	G620 port	Connects to…
FC_switch_B_2	B	8	25	49	19	controller_B_3 port FC-VI d
FC_switch_B_2	B	8	28	52	22	controller_B_4 port FC-VI b
FC_switch_B_2	B	8	29	53	23	controller_B_4 port FC-VI d

Zone in Fabric_2	Member ports
QOSH2_MC2_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
QOSH2_MC2_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

The following table provides a summary of the FC-VI zones:

Fabric	Zone name	Member ports
FC_switch_A_1 and FC_switch_B_1	QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
	QOSH2_MC1_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
	QOSH2_MC1_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53
FC_switch_A_2 and FC_switch_B_2	QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5
	QOSH2_MC1_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
	QOSH2_MC1_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

=== 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 grouplocation in pair

This portion of the name…	Identifies the…	Possible values…
site	Site on which the bridge pair physically resides.	A or B
stack group	Number of the stack group to which the bridge pair connects. • 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. • FibreBridge 6500N bridges support only a single stack in the stack group.	1, 2, etc.
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 for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_A_1	A	5	8	bridge_A_1a FC1
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c

Zone in Fabric_1
Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_A_1	A	6	8	bridge_A_1b FC1
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8

==== DR Group 1 - Stack 2 at Site_A

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	9	bridge_A_2a FC1
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_A_1	A	6	9	bridge_A_2b FC1
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9

==== DR Group 1 - Stack 1 at Site_B

MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:*

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c
FC_switch_B_1	B	7	8	bridge_B_1a FC1

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch	Connects to…
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d
FC_switch_B_1	B	8	8	bridge_B_1b FC1

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1 _BOT_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;8,8

==== DR Group 1 - Stack 2 at Site_B

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c
FC_switch_B_1	B	7	9	bridge_b_2a FC1

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_b_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d
FC_switch_B_1	B	8	9	bridge_B_1b FC1

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

==== Summary of storage zones

Fabric	Zone name	Member ports
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8
	vMC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

=== 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

This portion of the name…	Identifies the…	Possible values…

site	Site on which the bridge pair physically resides.	A or B
stack group	Number of the stack group to which the bridge pair connects. • 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. • FibreBridge 6500N bridges support only a single stack in the stack group.	1, 2, etc.
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 for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610/ G620 port	6520 port	Connects to…
FC_switch_A_1	A	5	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	controller_A_2 port 0a
FC_switch_A_1	A	5	8	8	bridge_A_1a FC1

FC switch	Site	Switch domain	6505 / 6510 / G610/ G620 port	6520 port	Connects to…
FC_switch_B_1	B	7	2	2	controller_B_1 port 0a
FC_switch_B_1	B	7	6	6	controller_B_2 port 0a

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_A_1	A	5	9	9	9	bridge_A_1b FC1
FC_switch_B_1	B	7	3	3	3	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	7	controller_B_2 port 0c

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610	6520	G620	Connects to…
FC_switch_A_2	A	6	2	2	2	controller_A_1 port 0b
FC_switch_A_2	A	6	6	6	6	controller_A_2 port 0b
FC_switch_A_2	A	6	8	8	8	bridge_A_1a FC2
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b
FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610	6520	G620	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0b
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0b
FC_switch_A_2	A	6	9	9	9	bridge_A_1b FC2
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b

FC switch	Site	Switch domain	6505 / 6510 / G610	6520	G620	Connects to…
FC_switch _B_2	B	8	7	7	7	controller_ B_2 port 0b

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_1 _BOT_FC2	6,3;6,7;8,3;8,7;6,9

==== DR Group 1 - Stack 2 at Site_A

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch _A_1	A	5	2	2	2	controller_ A_1 port 0a
FC_switch _A_1	A	5	6	6	6	controller_ A_2 port 0a
FC_switch _A_1	A	5	10	10	10	bridge_A_ 2a FC1
FC_switch _B_1	B	7	2	2	2	controller_ B_1 port 0a
FC_switch _B_1	B	7	6	6	6	controller_ B_2 port 0a

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2 _TOP_FC1	5,2;5,6;7,2;7,6;5,10

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_A_1	A	5	11	11	11	bridge_A_2b FC1
FC_switch_B_1	B	7	3	3	3	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	7	controller_B_2 port 0c

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	2	0	0	controller_A_1 port 0b
FC_switch_A_2	A	6	6	4	4	controller_A_2 port 0b
FC_switch_A_2	A	6	10	10	10	bridge_A_2a FC2
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch _B_2	B	8	6	6	6	controller_ B_2 port 0b

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2 _TOP_FC2	6,2;6,6;8,2;8,6;6,10

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch _A_2	A	6	3	3	3	controller_ A_1 port 0b
FC_switch _A_2	A	6	7	7	7	controller_ A_2 port 0b
FC_switch _A_2	A	6	11	11	11	bridge_A_ 2b FC2
FC_switch _B_2	B	8	3	3	3	controller_ B_1 port 0b\
FC_switch _B_2	B	8	7	7	7	controller_ B_2 port 0b

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_2 _BOT_FC2	6,3;6,7;8,3;8,7;6,11

==== DR Group 1 - Stack 1 at Site_B

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	2	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	6	controller_A_2 port 0a
FC_switch_B_1	B	7	2	2	8	controller_B_1 port 0a
FC_switch_B_1	B	7	6	6	2	controller_B_2 port 0a
FC_switch_B_1	B	7	8	8	6	bridge_B_1a FC1

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

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_B_1	B	7	3	3	9	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	3	controller_B_2 port 0c

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_B_1	B	7	9	9	7	bridge_B_1b FC1

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

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	2	2	2	controller_A_1 port 0b
FC_switch_A_2	A	6	6	6	6	controller_A_2 port 0b
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b
FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b
FC_switch_B_2	B	8	8	8	8	bridge_B_1a FC2

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0b
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0b
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b
FC_switch_B_2	B	8	7	7	7	controller_B_2 port 0b
FC_switch_B_2	B	8	9	9	9	bridge_A_1b FC2

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9

==== DR Group 1 - Stack 2 at Site_B

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	2	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	6	controller_A_2 port 0a
FC_switch_B_1	B	7	2	2	2	controller_B_1 port 0a

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_B_1	B	7	6	6	6	controller_B_2 port 0a
FC_switch_B_1	B	7	10	10	10	bridge_B_2a FC1

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_B_1	B	7	3	3	3	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	7	controller_B_2 port 0c
FC_switch_B_1	B	7	11	11	11	bridge_B_2b FC1

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

Table for DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	2	2	2	controller_A_1 port 0b
FC_switch_A_2	A	6	6	6	6	controller_A_2 port 0b
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b
FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b
FC_switch_B_2	B	8	10	10	10	bridge_B_2a FC2

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10

Table for DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0b
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0b
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b
FC_switch_B_2	B	8	7	7	7	controller_B_2 port 0b

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_B_2	B	8	11	11	11	bridge_B_2b FC2

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

==== Summary of storage zones

Fabric		Zone name	Member ports
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10
FC_switch_A_1 FC_switch_B_1	and	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11
FC_switch_A_2 FC_switch_B_2	and	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8
FC_switch_A_2 FC_switch_B_2	and	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9
FC_switch_A_2 FC_switch_B_2	and	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10

Fabric	Zone name	Member ports
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_A _STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_B _STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_B _STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_B _STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_B _STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

=== 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.

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

Zoning for FC-VI ports

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

Zoning for FibreBridge 7500N bridges using both FC ports

1. Create the FC-VI zones on each switch: `zonecreate "QOSH1_FCVI_1", member;member ...`

   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 ...`

      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...`

   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_namezone;zone...`

d. Enable the configuration: `cfgenable config_name`

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

e. Save the configuration: `cfgsave`

```
Switch_A_1:admin> cfgsave
```

f. Validate the zoning configuration: `zone --validate`

```
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.

- You must have Brocade 6510 or G620 switches.

  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.

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.

1. Disable the virtual fabric by entering the following command at the switch console:`fosconfig --disable vf`

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.

The data field size must not exceed 2048.

1. Disable the switch: `switchdisable`
2. Configure and set the payload: `configure`
3. Set the following switch parameters:
   a. Set the Fabric parameter as follows: `y`
   b. Set the other parameters, such as Domain, WWN Based persistent PID, and so on.
   c. Set the data field size: `2048`

=== Setting the authentication policy

You must set the authentication policy and associated parameters.

The commands must be executed at the switch console.

1. Set the authentication secret:
   a. Begin the setup process: `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.

   The following is an example of setting the authentication secret:

   +

```
brcd> secAuthSecret --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.

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

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

   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`

   The following example shows that encryption is enabled on ports 8 and 12:

```
User Encryption
Port  configured     Active
----   ----------    ------
 8      yes          yes
 9      No           No
 10     No           No
 11     No           No
 12     yes          yes
```

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

= Configuring the Cisco FC switches :icons: font

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

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.

  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.

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.

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.

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

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.

The following example shows the process on a fabric consisting of FC_switch_A_1 and FC_switch_B_1.

```
FC_Switch_A_1# write erase
    Warning: This command will erase the startup-
configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_A_1# reload
    This command will reboot the system. (y/n)?  [n] y

FC_Switch_B_1# write erase
    Warning: This command will erase the startup-
configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_B_1# reload
    This command will reboot the system. (y/n)?  [n] y
```

== 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.

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.

   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.

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.

- 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.

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 tinterface port_numbershutport-license acquireno shut`

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.

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
- Port assignments for FC switches when using ONTAP 9.0

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

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:

```
Switch_A_1# config  t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config  t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

== 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.

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.

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 fcrxbbcredit 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 fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_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.

The examples here use the following naming conventions:

Switch fabric	VSAN name	ID number
1	FCVI_1_10	10
STOR_1_20	20	2
FCVI_2_30	30	STOR_2_20

This task must be performed on each FC switch fabric.

1. Configure the FC-VI VSAN:
   a. Enter configuration mode if you have not done so already: `config 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`

   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
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

3. Verify port membership of the VSAN: `show vsan member`

```
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:

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

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

- The following steps must be performed to configure in-order delivery of frames:
  i. Enter configuration mode: `conf t`
  ii. Enable the in-order guarantee of exchanges for the VSAN: `in-order-guarantee vsan vsan-ID`

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.

  iii. Enable load balancing for the VSAN: `vsan vsan-ID loadbalancing src-dst-id`
  iv. Exit configuration mode: `end`
  v. Copy the running-config to the startup-config: `copy running-config startup-config`

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

```
FC_switch_B_1# config t
FC_switch_B_1(config)# 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
```

- The following steps must be performed to configure out-of-order delivery of frames:
  i. Enter configuration mode: `conf t`
  ii. Disable the in-order guarantee of exchanges for the VSAN: `no in-order-guarantee vsan vsan-ID`
  iii. Enable load balancing for the VSAN: `vsan vsan-ID loadbalancing src-dst-id`
  iv. Exit configuration mode: `end`
  v. 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
```

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

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: `priority high`

   e. Add the VSAN to the policy map created previously in this procedure: `qos service policy policy_name vsan vsanid`

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

   The commands to set the QoS policies on FC_switch_A_1:

   +

```
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)# 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:

+

```
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)# 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: `vsan vsan-ID`

   b. Set the VSAN name: `vsan vsan-ID name vsan_name`

   The commands to configure 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-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:

+

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

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.

   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).

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

This task must be performed on each ISL port.

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.

Speed in Gbps	BBCs required per kilometer	Adjusted BBCs required (BBCs per km x 1.5)
1	0.5	0.75
2	1	1.5
4	2	3

8	4	6
16	8	12

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 fcrxbbcredit 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 10switchport 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.

    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).

```
FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
    Hardware is Fibre Channel
    Port WWN is 24:01:54:7f:ee:e2:8d:a0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,10,20)
    Trunk vsans (up)                       (1,10,20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 1154832 bits/sec,144354
bytes/sec, 170 frames/sec
    5 minutes output rate 1299152 bits/sec,162394
bytes/sec, 183 frames/sec
      535724861 frames input,1069616011292 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      572290295 frames output,1144869385204 bytes
        0 discards,0 errors
      5 input OLS,11  LRR,2 NOS,0 loop inits
      14 output OLS,5 LRR, 0 NOS, 0 loop inits
    Member[1] : fc1/36
    Member[2] : fc1/40
    Interface last changed at Thu Oct 16 11:48:00 2014
```

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`

```
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
```

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

Related information

Port assignments for FC switches when using ONTAP 9.1 and later

=== 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.

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.

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

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

   +

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

The following example shows the configuration of the FCIP profile:

+

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

The following example shows the configuration of the FCIP profile:

+

```
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 pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

6. Create the first of two FCIP interfaces: `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 26to mark all packets on that differentiated services code point (DSCP) value: `qos control 48 data 26`

   g. Exit the interface configuration mode: `exit`

The following example shows the configuration of the FCIP interface:

+

```
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
```

1. 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 26to mark all packets on that differentiated services code point (DSCP) value: `qos control 48 data 26`

   g. Exit the interface configuration mode: `exit`

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
```

1. 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`

2. 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`

3. 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.

4. Restart the ports on both switches: `no shutdown`

5. Exit the interface configuration on both switches: `end`

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

```
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
```

7. 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.

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.

[fcip ports dual isl] | *./install-fc/../media/../media/fcip_ports_dual_isl.gif*

The task and examples use the following profile configuration table:

Switch fabric	IPStorage interface	IP Address	Port type	FCIP interface	FCIP profile	Port	Peer IP/port	VSAN ID
Fabric 1	FC_switch_A_1	IPStorage1/1	a.a.a.a	FC-VI	fcip 1	15	3220	c.c.c.c/3230
10	Fabric 1	FC_switch_A_1	IPStorage1/1	a.a.a.a	Storage	fcip 2	20	3221
	20	Fabric 1	FC_switch_A_1	IPStorage1/2	b.b.b.b	FC-VI	fcip 3	25
3222	d.d.d.d/3232	10	Fabric 1	FC_switch_A_1	IPStorage1/2	b.b.b.b	Storage	fcip 4
30	3223	d.d.d.d/3233	20	FC_switch_B_1	IPStorage1/1	c.c.c.c	FC-VI	fcip 1
15	3230	a.a.a.a/3220	10	FC_switch_B_1	IPStorage1/1	c.c.c.c	Storage	fcip 2
20	3231	a.a.a.a/3221	20	FC_switch_B_1	IPStorage1/2	d.d.d.d	FC-VI	fcip 3
25	3232	b.b.b.b/3222	10	FC_switch_B_1	IPStorage1/2	d.d.d.d	Storage	fcip 4
30	3233	b.b.b.b/3223	20	Fabric 2	FC_switch_A_2	IPStorage1/1	e.e.e.e	FC-VI
fcip 1	15	3220	g.g.g.g/3230	10	Fabric 2	FC_switch_A_2	IPStorage1/1	e.e.e.e
Storage	fcip 2	20	3221	g.g.g.g/3231	20	Fabric 2	FC_switch_A_2	IPStorage1/2

Switch fabric	IPStorage interface	IP Address	Port type	FCIP interface	FCIP profile	Port	Peer IP/port	VSAN ID
f.f.f.f	FC-VI	fcip 3	25	3222	h.h.h.h/3232	10	Fabric 2	FC_switch_A_2
IPStorage1/2	f.f.f.f	Storage	fcip 4	30	3223	h.h.h.h/3233	20	FC_switch_B_2
IPStorage1/1	g.g.g.g	FC-VI	fcip 1	15	3230	e.e.e.e/3220	10	FC_switch_B_2
IPStorage1/1	g.g.g.g	Storage	fcip 2	20	3231	e.e.e.e/3221	20	FC_switch_B_2
IPStorage1/2	h.h.h.h	FC-VI	fcip 3	25	3232	f.f.f.f/3222	10	FC_switch_B_2

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-addresssubnet-mask`

      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: `exit`
   g. Repeat steps a through f 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 1tcp max-retransmissions 3max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms 3tcp min-retransmit-time 200tcp keepalive-timeout 1tcp pmtu-enable reset-timeout 3600tcp 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 ipaddrpeer 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 26to 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
conf 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

conf 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
  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 <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.

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

1. Clear the existing zones and zone set, if present.

   a. Determine which zones and zone sets are active: `show zoneset active`

   ```
   FC_switch_A_1# show zoneset active

   FC_switch_B_1# show zoneset active
   ```

   b. Disable the active zone sets identified in the previous step: `no zoneset activate name zoneset_name vsan vsan_id`

   The following example shows two zone sets being disabled:

   - ZoneSet_A on FC_switch_A_1 in VSAN 10
   - ZoneSet_B on FC_switch_B_1 in VSAN 20

```
FC_switch_A_1# no zoneset activate name ZoneSet_A vsan
10

FC_switch_B_1# no zoneset activate name ZoneSet_B vsan
20
```

a. After all zone sets are deactivated, clear the zone database: `clear zone database zone-name`

```
FC_switch_A_1# clear zone database 10
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# clear zone database 20
FC_switch_B_1# copy running-config startup-config
```

2. Obtain the switch worldwide name (WWN): `show wwn switch`
3. Configure the basic zone settings:
   a. Set the default zoning policy to 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`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone
default-zone permit
FC_switch_A_1(config)# system default zone distribute
full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan
10
FC_switch_A_1(config)# zoneset distribute full vsan
20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone
default-zone permit
FC_switch_B_1(config)# system default zone distribute
full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan
10
FC_switch_B_1(config)# zoneset distribute full vsan
20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

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
   - Zoning for FibreBridge 7500N bridges using both FC ports 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 portswitch WWN`
     c. Activate the zone set: `zoneset activate name STOR_zonenameesetname vsan vsanid`

```
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 fc1/5 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 a storage zone set and add the storage zones to the new set.

   You only need to perform these steps on one switch in the fabric.

   a. Create the storage zone set: `zoneset name STOR_zonesetname vsan vsanid`

   b. Add storage zones to the zone set: `member STOR_zonename`

   c. Activate the zone set: `zoneset activate name STOR_zonesetname vsan vsanid`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name
STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member
STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name
STOR_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. Create FCVI zones and add the FCVI ports to them.

   Each FCVI zone contains the FCVI ports from all the controllers of one DR Group.

   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
   - Zoning for FibreBridge 7500N bridges using both FC ports Each storage zone contains the HBA initiator ports from all controllers and one single port connecting an FC-to-SAS bridge.
     a. Create the FCVI zones: `zone name FCVI_zone-name vsan vsanid`
     b. Add FCVI ports to the zone: `member FCVI zone-name`
     c. Activate the zone set: `zoneset activate name FCVI_zonenameesetname vsan vsanid`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan
10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

7. Create an FCVI zone set and add the FCVI zones 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`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10
vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
    ...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name
FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

8. Verify the zoning: `show zone`

9. 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.

1. Issue the following command on both FC switch fabrics:`copy running-config startup-config`

```
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# copy running-config startup-config
```

= Installing FC-to-SAS bridges and SAS disk shelves :icons: font

You install and cable ATTO FibreBridge bridges and SAS disk shelves when adding new storage to the configuration.

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:

[workflow bridge installation and configuration] | *./install-*

fc/../media/../media/workflow_bridge_installation_and_configuration.gif

== 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. Beginning with ONTAP 9.8, out-of-band management is deprecated.

> Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

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.

The availability of in-band management of the bridges depends on the version of ONTAP:

- Starting with ONTAP 9.8, bridges are managed via in-band connections by default and out-of-band management of the bridges via SNMP is deprecated.
- ONTAP 9.5 through 9.7: Either in-band management or out-of-band SNMP management is supported.
- Prior to ONTAP 9.5, only out-of-band SNMP management is supported.

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

> 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.

- 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.

- 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.

  1. Download the *Installation and Service Guide* for your disk shelf model:
  2. Access the ATTO web site using the link provided for your FibreBridge model and download the manual and the QuickNAV utility.

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

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

  3. Gather the hardware and information needed to use the recommended bridge management interfaces, the ATTO ExpressNAV GUI, and the ATTO QuickNAV 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 QuickNAV 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.

- 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.

> 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 IOM3 modules is not supported within the same storage stack. A mix of IOM12 modules and IOM6 modules is supported within the same storage stack if your system is running a supported version of ONTAP.

> 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

> SAS shelves in MetroCluster configurations do not support ACP cabling.

=== 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.

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.

Starting with ONTAP 9.8, *in-band management* of the bridges is supported by default and out-of-band SNMP management is deprecated.

This task is required if you are **not** using in-band management to manage the bridges. In this case, you need to configure the bridge via the Ethernet management port.

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 a service, if desired, by issuing the set closeport and repeating the command as necessary until all desired services are disabled: `set closeport service`

   The set closeport command disables a single service at a time.

   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.

4. If you are enabling SNMP, you must also issue the set SNMP enabled command: `set SNMP enabled`

   SNMP is the only protocol that requires a separate enable command.

5. Save the configuration: `saveconfiguration`

=== 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.

You should decide whether you will be using in-band management of the bridges.

Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

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.

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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

   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.

   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 the Ethernet port. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

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

      If using the CLI, you must run the following commands:`set ipaddress mp1 ip-addressset ipsubnetmask mp1 subnet-maskset ipgateway mp1 x.x.x.xset ipdhcp mp1 disabled``set ethernetspeed mp1 1000`

   b. Configure the bridge name.

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

      Example bridge names for one stack group on each site:

      - bridge_A_1a
      - bridge_A_1b

- bridge_B_1a
- bridge_B_1b If using the CLI, you must run the following command:`set bridgename bridgename`

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

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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

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 to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

If using the CLI, you must run the following command: `set FCDataRate port-numberport-speed`

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

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

If using the CLI, you must run the following command: `set FCConnMode port-number ptp`

b. 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`

The following example shows the disabling of FC port 2:

```
`FCPortDisable 2`

Fibre Channel Port 2 has been disabled.
```

c. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports: `SASPortDisable sas-port``

   SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used.

   If only SAS port A is used, then SAS ports B, C, and D must be disabled. The following example shows the disabling of SAS port B. You must similarly disable SAS ports C and D:

   ```
   SASPortDisable b
   ```

   SAS Port B has been disabled.

6. Secure access to the bridge and save the bridge's configuration. Choose an option from below depending on the version of ONTAP your system is running.

ONTAP version	Steps
ONTAP 9.5 or later	a. View the status of the bridges: `storage bridge show` The output shows which bridge is not secured. b. Secure the bridge: `securebridge`

ONTAP 9.4 or earlier	a. View the status of the bridges: `storage bridge show`
	
	The output shows which bridge is not secured.
	
	b. Check the status of the unsecured bridge's ports: info
	
	The output shows the status of Ethernet ports MP1 and MP2.
	
	c. If Ethernet port MP1 is enabled, run: `set EthernetPort mp1 disabled`
	
	If Ethernet port MP2 is also enabled, repeat the previous substep for port MP2.
	
	d. Save the bridge's configuration.
	
	You must run the following commands:
	
	`SaveConfiguration`
	
	`FirmwareRestart`
	
	You are prompted to restart the bridge.

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.

   Maintain MetroCluster Components

Related information

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

=== Cabling disk shelves to the bridges

You must use the correct FC-to-SAS bridges for cabling your disk shelves.

==== Cabling a FibreBridge 7600N or 7500N bridge with disk shelves using IOM12 modules

After configuring the bridge, you can start cabling your new system.

For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

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.

   - 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).

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.

   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:

   +

   [mcc cabling bridge and sas3 stack with 7500n and multiple stacks] | *./install-*

fc/../media/../media/mcc_cabling_bridge_and_sas3_stack_with_7500n_and_multiple

_stacks.gif

==== 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.

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).

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:

   + image::../install-fc/../media/../media/mcc_cabling_bridge_and_sas_stack_with_7500n_and_single_stack.gif[]

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.

   [mcc cabling bridge and sas stack with 7500n four stacks] | *../install-*

fc/../media/../media/mcc_cabling_bridge_and_sas_stack_with_7500n_four_stacks.gif

==== 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.

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.

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.

   The SAS port B bridge is disabled.

   The following illustration shows a set of bridges cabled to a stack of four disk shelves:

   [mcc cabling bridge and sas stack] | *./install-*

fc/../media/../media/mcc_cabling_bridge_and_sas_stack.gif

=== 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.

1. Verify that each bridge can detect all of the disk drives and disk shelves it is connected to:

If you are using the…	Then…
ATTO ExpressNAV GUI	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. 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. c. Click **Advanced**. d. View the connected devices by using the sastargets command, and then click **Submit**.
Serial port connection	View the connected devices: `sastargets`

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:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK
3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK
3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK
3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK
3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK
3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK
3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK
3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK
3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK
3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK
3QP1FXW600009940VERQ
```

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.

If the output is…	Then…
Correct	Repeat Step 1 for each remaining bridge.
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating the cabling. Cabling disk shelves to the bridges b. Repeat Step 1.

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:

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 information

Port assignments for FC switches when using ONTAP 9.1 and later

Port assignments for FC switches when using ONTAP 9.0

== Securing or unsecuring the FibreBridge bridge

To easily disable potentially unsecure Ethernet protocols on a bridge, beginning with ONTAP 9.5 you can secure the bridge. This disables the bridge's Ethernet ports. You can also reenable Ethernet access.

- 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.
- In ONTAP 9.7 and earlier, running the `securebridge` command on the ATTO FibreBridge might not update the bridge status correctly on the partner cluster. If this occurs, run the `securebridge` command from the partner cluster.

Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

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

   The following command secures bridge_A_1:

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

   The following command unsecures bridge_A_1:

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

2. From the ONTAP prompt of the cluster containing the bridge, save the bridge

configuration: `storage bridge run-cli -bridge bridge-name -command saveconfiguration`

The following command secures bridge_A_1:

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

   The following command secures bridge_A_1:

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