Configure the MetroCluster hardware components

ONTAP MetroCluster

NetApp
February 07, 2022

Table of Contents

Configure the MetroCluster hardware components

Parts of a MetroCluster IP configuration

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

Key hardware elements

A MetroCluster IP configuration includes the following key hardware elements:

- Storage controllers

  The storage controllers are configured as two two-node clusters.

- IP network

  This back-end IP network provides connectivity for two distinct uses:

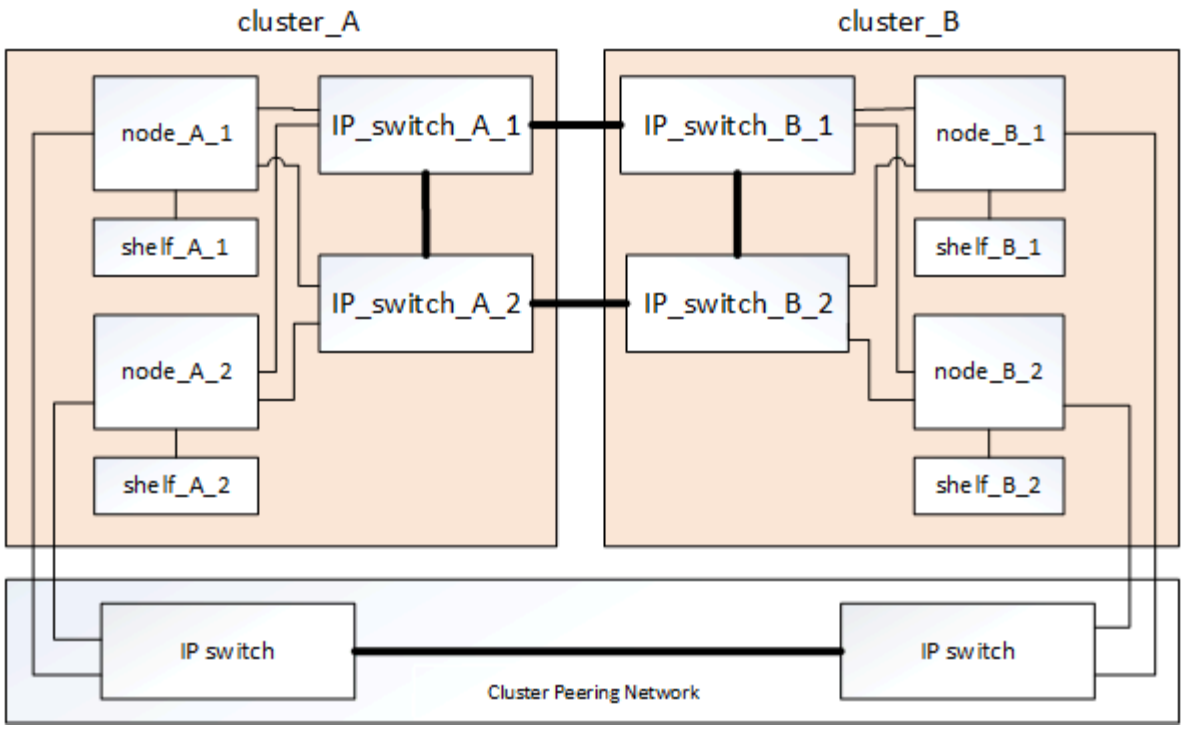
  - Standard cluster connectivity for intra-cluster communications.

    This is the same cluster switch functionality used in non-MetroCluster switched ONTAP clusters.

  - MetroCluster back-end connectivity for replication of storage data and non-volatile cache.

- 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.



Disaster Recovery (DR) groups

A MetroCluster IP configuration consists of one DR group of four nodes.

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

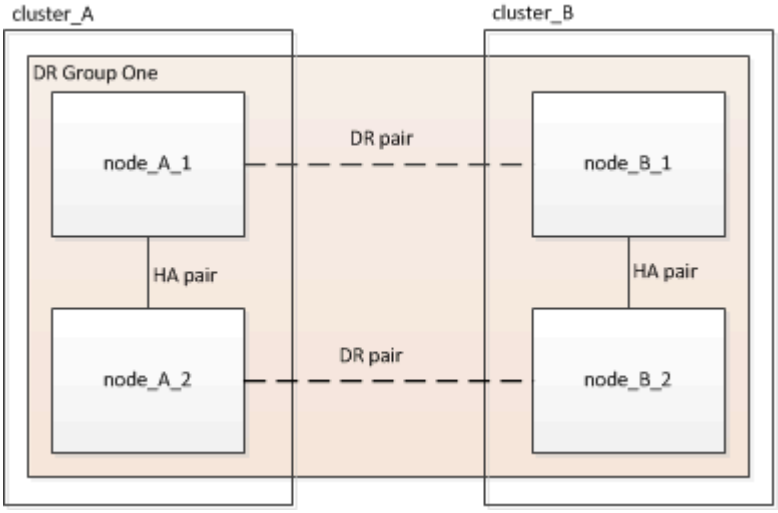
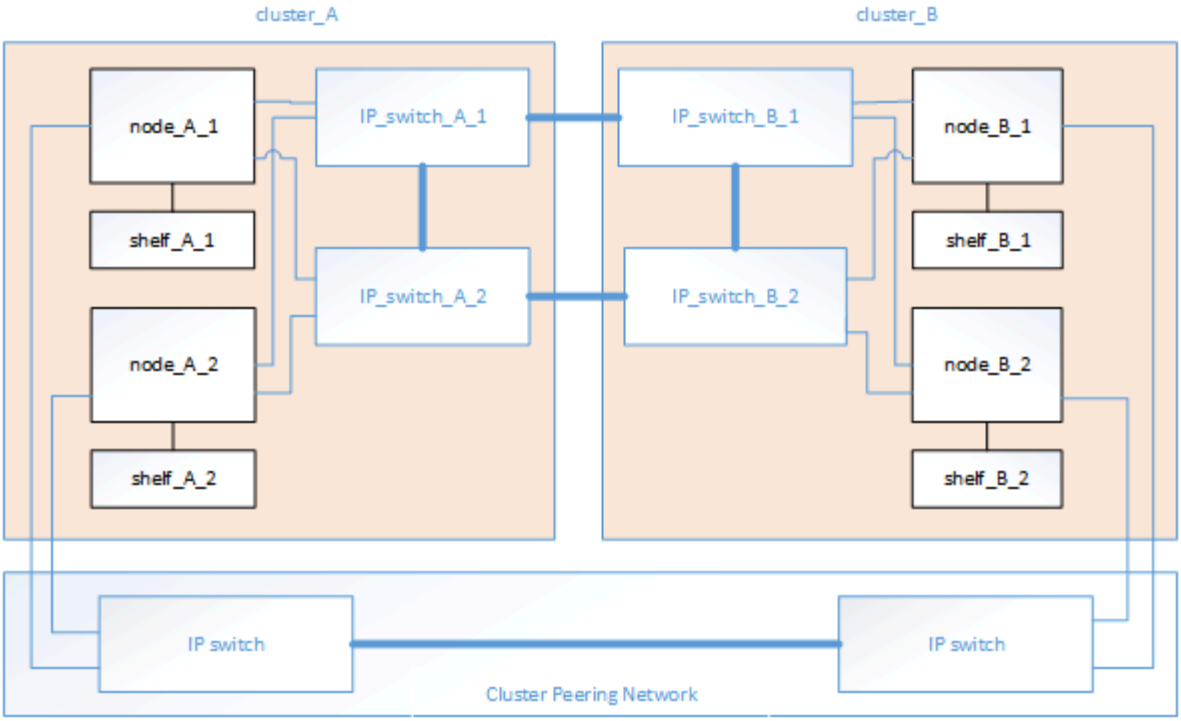


Illustration of the local HA pairs in a MetroCluster configuration

Each MetroCluster site consists of storage controllers configured as an HA pair. 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.

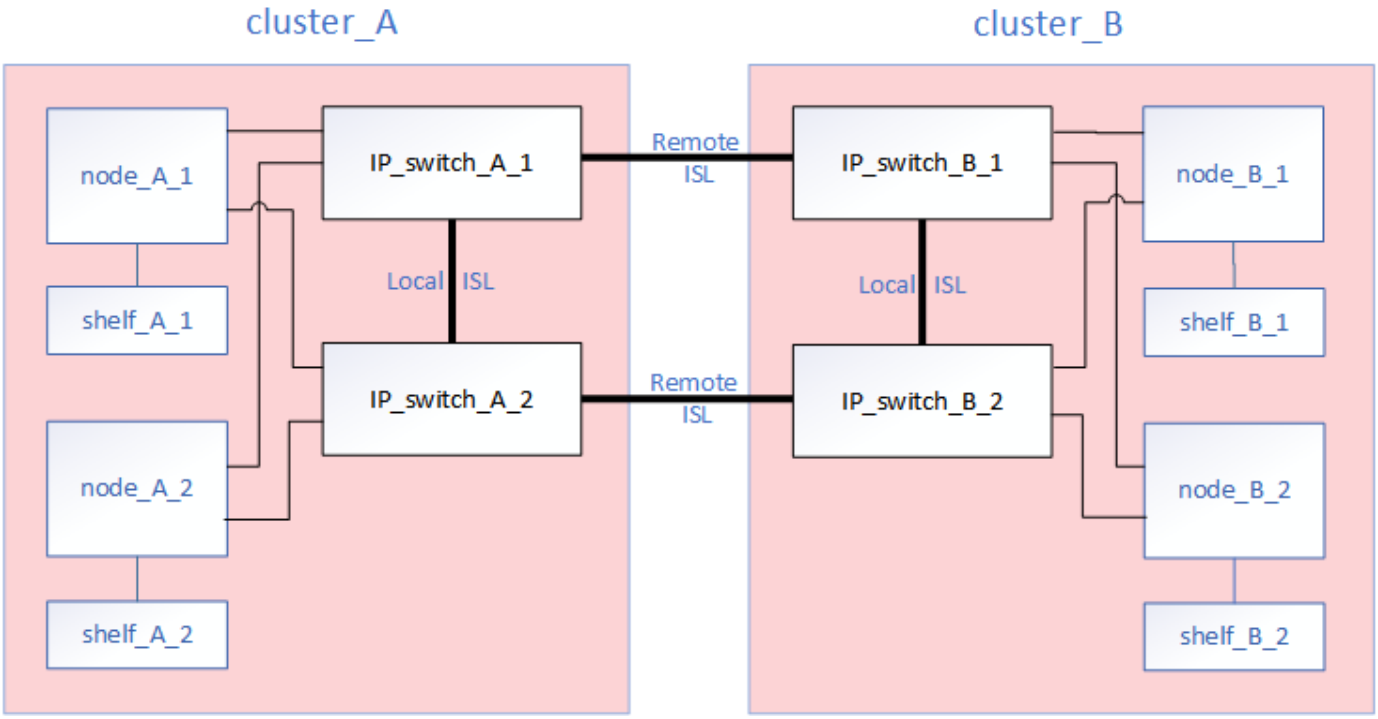


Related information

ONTAP concepts

Illustration of the MetroCluster IP and cluster interconnect network

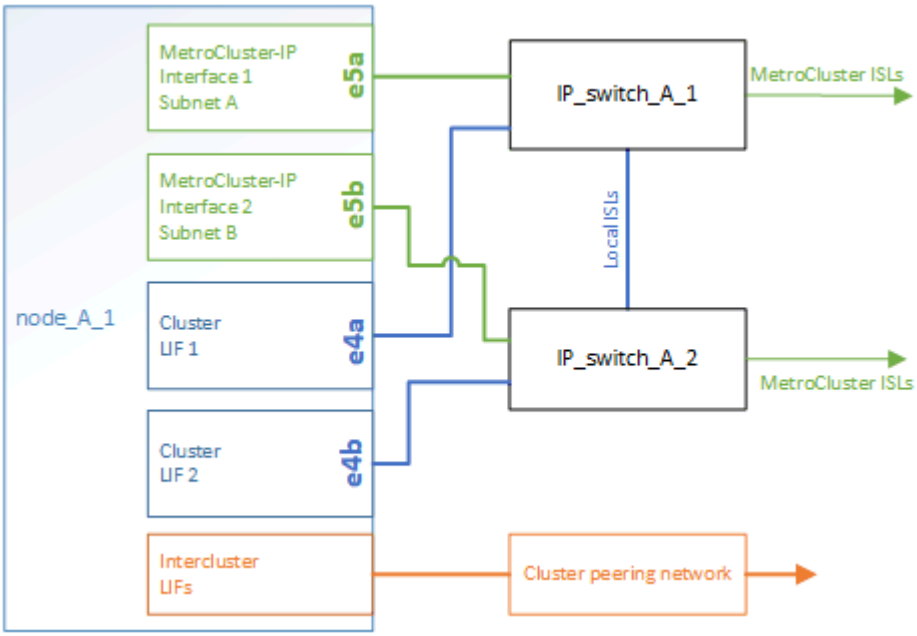
ONTAP clusters typically include a cluster interconnect network for traffic between the nodes in the cluster. In MetroCluster IP configurations, this network is also used for carrying data replication traffic between the MetroCluster sites.



Each node in the MetroCluster IP configuration has specialized LIFs for connection to the back-end IP network:

- Two MetroCluster IP interfaces
- One intercluster LIF

The following illustration shows these interfaces. The port usage shown is for an AFF A700 or FAS9000 system.



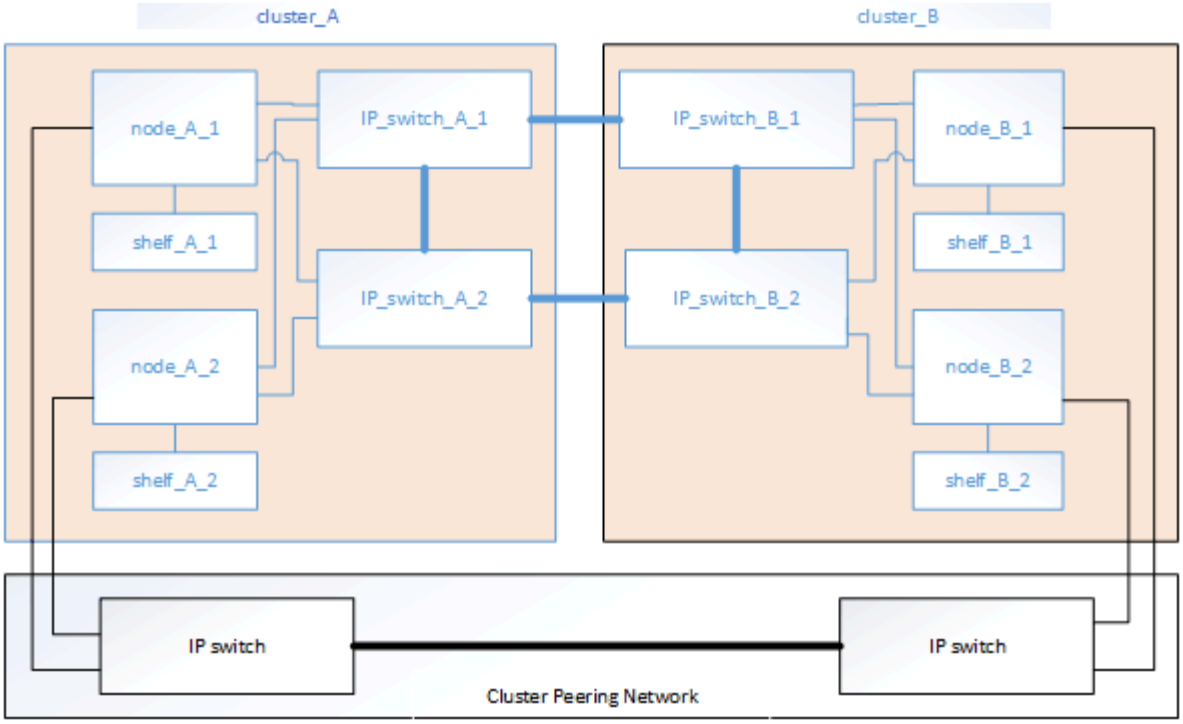
Related information

Considerations for MetroCluster IP configurations

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

Cluster and SVM peering express configuration

Considerations for configuring cluster peering

Cabling the cluster peering connections

Peering the clusters

Required MetroCluster IP components and naming conventions

When planning your MetroCluster IP 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.

Supported software and hardware

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

NetApp Hardware Universe

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

Hardware redundancy requirements in a MetroCluster IP configuration

Because of the hardware redundancy in the MetroCluster IP 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.

ONTAP cluster requirements in a MetroCluster IP configuration

MetroCluster IP configurations require 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

IP switch requirements in a MetroCluster IP configuration

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

The IP switches also provide intracluster communication among the controller modules in each cluster.

Naming must be unique within the MetroCluster configuration.

Example names:

- Site A: cluster_A
  - IP_switch_A_1
  - IP_switch_A_2
- Site B: cluster_B
  - IP_switch_B_1
  - IP_switch_B_2

Controller module requirements in a MetroCluster IP configuration

MetroCluster IP configurations require four or eight controller modules.

The controller modules at each site form an HA pair. Each controller module has a DR partner at the other site.

Each controller module must be running the same ONTAP version. Supported platform models depend on the ONTAP version:

- New MetroCluster IP installations on FAS systems are not supported in ONTAP 9.4.

  Existing MetroCluster IP configurations on FAS systems can be upgraded to ONTAP 9.4.

- Beginning with ONTAP 9.5, new MetroCluster IP installations on FAS systems are supported.
- Beginning with ONTAP 9.4, controller modules configured for ADP are supported.

Controller models limited to four-node configurations

These models are limited to four in a MetroCluster configuration.

- AFF A220
- AFF A250
- FAS2750
- FAS500f

For example, the following configurations are not supported:

- An eight-node configuration consisting of eight AFF A250 controllers.
- An eight-node configuration consisting of four AFF 220 controllers and four FAS500f controllers.
- Two four-node MetroCluster IP configurations each consisting of AFF A250 controllers and sharing the same back-end switches.
- An eight-node configuration consisting of DR Group 1 with AFF A250 controllers and DR Group 2 with FAS9000 controllers.

You can configure two separate four-node MetroCluster IP configurations with the same back-end switches if the second MetroCluster does not include any of the above models.

Example names

The following example names are used in the documentation:

- Site A: cluster_A
  - controller_A_1
  - controller_A_2
- Site B: cluster_B
  - controller_B_1
  - controller_B_2

Gigabit Ethernet adapter requirements in a MetroCluster IP configuration

MetroCluster IP configurations use a 40/100 Gbps or 10/25 Gbps Ethernet adapter for the IP interfaces to the IP switches used for the MetroCluster IP fabric.

Platform model	Required Gigabit Ethernet adapter	Required slot for adapter	Ports
AFF A900	X91146A	Slot 5, Slot 7	e5b, e7b
AFF A700 and FAS9000	X91146A-C	Slot 5	e5a, e5b
AFF A800	X1146A/onboard ports	Slot 1	e0b. e1b
AFF A400 and FAS8300	X1146A	Slot 1	e1a, e1b
AFF A300 and FAS8200	X1116A	Slot 1	e1a, e1b
AFF A220, and FAS2750	Onboard ports	Slot 0	e0a, e0b

AFF A250 and FAS500f	Onboard ports	Slot 0	e0c, e0d
AFF A320	Onboard ports	Slot 0	e0g, e0h

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.

A four-node MetroCluster IP configuration requires the minimum configuration at each site:

- Each node has at least one local pool and one remote pool at the 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.

Drive location considerations for AFF A800 internal drives

For correct implementation of the ADP feature, the AFF A800 system disk slots must be divided into quarters and the disks must be located symmetrically in the quarters.

An AFF A800 system has 48 drive bays. The bays can be divided into quarters:

- Quarter one:
  - Bays 0 - 5
  - Bays 24 - 29
- Quarter two:
  - Bays 6 - 11
  - Bays 30 - 35

- Quarter three:
  - Bays 12 - 17
  - Bays 36 - 41
- Quarter four:
  - Bays 18 - 23
  - Bays 42 - 47

If this system is populated with 16 drives, they must be symmetrically distributed among the four quarters:

- Four drives in the first quarter: 0, 1, 2, 3
- Four drives in the second quarter: 6, 7, 8, 9
- Four drives in the third quarter: 12, 13, 14, 15
- Four drives in the fourth quarter: 18, 19, 20, 21

Mixing IOM12 and IOM 6 modules in a stack

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

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

Racking the hardware components

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

About this task

This task must be performed on both MetroCluster sites.

Steps

1. Plan out the positioning of the MetroCluster components.

   The rack space depends on the platform model of the controller modules, the switch types, and the number of disk shelf stacks in your configuration.

2. Properly ground yourself.

3. Install the controller modules in the rack or cabinet.

   AFF A220/FAS2700 Systems Installation and Setup Instructions

   AFF A250 Systems Installation and Setup Instructions

   AFF A300 Systems Installation and Setup Instructions

   AFF A320 systems: Installation and setup

   AFF A400 Systems Installation and Setup Instructions

AFF A700 Systems Installation and Setup Instructions

AFF A800 Systems Installation and Setup Instructions

FAS500f Systems Installation and Setup Instructions

FAS8200 Systems Installation and Setup Instructions

FAS8300 and FAS8700 Systems Installation and Setup Instructions

FAS9000 Systems Installation and Setup Instructions

1. Install the IP switches in the rack or cabinet.
2. 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).

> Do not cable disk shelves intended to contain unmirrored aggregates at this time. You must wait to deploy shelves intended for unmirrored aggregates until after the MetroCluster configuration is complete and only deploy them after using the `metrocluster modify -enable-unmirrored-aggr-deployment true` command.

Cable the MetroCluster IP switches

Using the port tables with the RcfFileGenerator tool or multiple MetroCluster configurations

You must understand how to use the information in the port tables to correctly generate your RCF files.

Before you begin

Review these considerations before using the tables:

- The following tables show the port usage for site A. The same cabling is used for site B.
- The switches cannot be configured with ports of different speeds (for example, a mix of 100 Gbps ports and 40 Gbps ports).
- Keep track of the MetroCluster port group (MetroCluster 1, MetroCluster 2, etc.). You will need this information when using the RcfFileGenerator tool as described later in this configuration procedure.
- The RcfFileGenerator for MetroCluster IP also provides a per-port cabling overview for each switch. Use this cabling overview to verify your cabling.

Cabling eight-node MetroCluster configurations

For MetroCluster configuration running ONTAP 9.8 and earlier, some procedures that are performed to transition an upgrade require the addition of a second four-node DR group to the configuration to create a temporary eight-node configuration. Beginning with ONTAP 9.9.1, permanent 8-node MetroCluster configurations are supported.

About this task

For such configurations, you use the same method as described above. Instead of a second MetroCluster, you are cabling an additional four-node DR group.

For example, your configuration includes the following:

- Cisco 3132Q-V switches
- MetroCluster 1: FAS2750 platforms
- MetroCluster 2: AFF A700 platforms (these platforms are being added as a second four-node DR group)

Steps

1. For MetroCluster 1, cable the Cisco 3132Q-V switches using the table for the FAS2750 platform and the rows for MetroCluster 1 interfaces.
2. For MetroCluster 2 (the second DR group), cable the Cisco 3132Q-V switches using the table for the AFF A700 platform and the rows for MetroCluster 2 interfaces.

Platform port assignments for Cisco 3132Q-V switches

The port usage in a MetroCluster IP configuration depends on the switch model and platform type.

Port usage for FAS2750 or AFF A220 systems and a Cisco 3132Q-V switch

Cabling an AFF A220 or FAS2750 to a Cisco 3132Q-V switch			
Port use	FAS2750. AFF A220		Switch Port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1
			2
			3
			4
			5
			6
ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	9/1
	disabled		9/2-4
	e0a	e0b	10/1
	disabled		10/2-4
MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	11/1
	disabled		11/2-4
	e0a	e0b	12/1
	disabled		12/2-4
MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	13/1
	disabled		13/2-4
	e0a	e0b	14/1
	disabled		14/2-4
ISL, MetroCluster native speed 40G	ISL, MetroCluster		15 - 20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Port usage for FAS9000, AFF A700 and a Cisco 3132Q-V switch

Cabling an AFF A700 or FAS9000 to a Cisco 3132Q-V switch			
Port use	FAS9000, AFF A700		Switch port
	IP_switch_x_1	IP_switch_x_2	Port
MetroCluster 1 Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2 Local Cluster interface			3
			4
MetroCluster 3 Local Cluster interface			5
			6
ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster		7
			8
MetroCluster 1 MetroCluster interface	e5a	e5b	9
	e5a	e5b	10
MetroCluster 2 MetroCluster interface	e5a	e5b	11
	e5a	e5b	12
MetroCluster 3 MetroCluster interface	e5a	e5b	13
	e5a	e5b	14
ISL, MetroCluster native speed 40G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Port usage for AFF A800 and a Cisco 3132Q-V switch

Cabling an AFF A800 to a Cisco 3132Q-V switch			
Port use	AFF A800		Switch Port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1 Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2 Local Cluster interface			3
			4
MetroCluster 3 Local Cluster interface			5
			6
ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster		7
			8
MetroCluster 1 MetroCluster interface	e0b	e1b	9
	e0b	e1b	10
MetroCluster 2 MetroCluster interface	e0b	e1b	11
	e0b	e1b	12
MetroCluster 3 MetroCluster interface	e0b	e1b	13
	e0b	e1b	14
ISL, MetroCluster native speed 40G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Platform port assignments for Cisco 3232C or Cisco 9336C switches

The port usage in a MetroCluster IP configuration depends on the switch model and platform type.

Review these considerations before using the tables:

- The following tables show the port usage for site A. The same cabling is used for site B.
- The switches cannot be configured with ports of different speeds (for example, a mix of 100 Gbps ports and 40 Gbps ports).
- If you are configuring a single MetroCluster with the switches, use the **MetroCluster 1** port group.

  Keep track of the MetroCluster port group (MetroCluster 1, MetroCluster 2, or MetroCluster 3). You will

need it when using the RcfFileGenerator tool as described later in this configuration procedure.

- The RcfFileGenerator for MetroCluster IP also provides a per-port cabling overview for each switch.

  Use this cabling overview to verify your cabling.

Cabling two MetroCluster configurations to the switches

When cabling more than one MetroCluster configuration to a Cisco 3132Q-V switch, then cable each MetroCluster according to the appropriate table. For example, if cabling a FAS2750 and an A700 to the same Cisco 3132Q-V switch. Then you cable the FAS2750 as per 'MetroCluster 1' in Table 1, and the A700 as per 'MetroCluster 2' or 'MetroCluster 3' in Table 2. You cannot physically cable both the FAS2750 and A700 as 'MetroCluster 1'.

Cabling a FAS2750 or AFF A220 system to a Cisco 3232C or Cisco 9336C switch

Cabling an AFF A220 or FAS2750 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS2750, AFF A220		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1 - 6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	9/1
	disabled		9/2-4
	e0a	e0b	10/1
	disabled		10/2-4
MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	11/1
	disabled		11/2-4
	e0a	e0b	12/1
	disabled		12/2-4
MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	13/1
	disabled		13/2-4
	e0a	e0b	14/1
	disabled		14/2-4
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Cabling a AFF A300 or FAS8200 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A300 or FAS8200 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS8200, AFF A300		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1 Local Cluster interface	See Hardware Universe for available ports		1/1
			1/2 - 4
			2/1
			2/2 - 4
MetroCluster 2 Local Cluster interface			3/1
			3/2 - 4
			4/1
			4/2 - 4
MetroCluster 3 Local Cluster interface			5/1
			5/2 - 4
			6/1
			6/2 - 4
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1 MetroCluster interface	e1a	e1b	9/1
	disabled		9/2-4
	e1a	e1b	10/1
	disabled		10/2-4
MetroCluster 2 MetroCluster interface	e1a	e1b	11/1
	disabled		11/2-4
	e1a	e1b	12/1
	disabled		12/2-4
MetroCluster 3 MetroCluster interface	e1a	e1b	13/1
	disabled		13/2-4
	e1a	e1b	14/1
	disabled		14/2-4
ISL, MetroCluster	ISL, MetroCluster		15 - 20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
MetroCluster 4 MetroCluster interface	e1a	e1b	25/1
	disabled		25/2-4
	e1a	e1b	26/1
	disabled		26/2-4
Unused	-		27 - 28
MetroCluster 4 Local Cluster interface	See Hardware Universe		29/1
	disabled		29/2-4
	See Hardware Universe		30/1
	disabled		30/2-4
Unused	-		31 - 32

Cabling a AFF A250 or FAS500f to a Cisco 3232C or Cisco 9336C switch

Cabling an AFF A250 or FAS500f to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS500f, AFF A250		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1 - 6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	9/1
	disabled		9/2-4
	e0c	e0d	10/1
	disabled		10/2-4
MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	11/1
	disabled		11/2-4
	e0c	e0d	12/1
	disabled		12/2-4
MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	13/1
	disabled		13/2-4
	e0c	e0d	14/1
	disabled		14/2-4
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Cabling a AFF A320 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A320 to a Cisco 3232C or Cisco 9336C switch			
Port use	AFF A320		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e0g	e0h	9
	e0g	e0h	10
MetroCluster 2, MetroCluster interface	e0g	e0h	11
	e0g	e0h	12
MetroCluster 3, MetroCluster interface	e0g	e0h	13
	e0g	e0h	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling an AFF A400, FAS8300 or FAS8700 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A400, FAS8300 or FAS8700 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS8300, FAS8700, AFF A400		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e1a	e1b	9
	e1a	e1b	10
MetroCluster 2, MetroCluster interface	e1a	e1b	11
	e1a	e1b	12
MetroCluster 3, MetroCluster interface	e1a	e1b	13
	e1a	e1b	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling a AFF A700 or FAS9000 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A700 or FAS9000 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS9000, AFF A700		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e5a	e5b	9
	e5a	e5b	10
MetroCluster 2, MetroCluster interface	e5a	e5b	11
	e5a	e5b	12
MetroCluster 3, MetroCluster interface	e5a	e5b	13
	e5a	e5b	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling a AFF A800 to a Cisco 3232C or Cisco 9336C switch

Cabling an AFF A800 to a Cisco 3232C or Cisco 9336C switch			
Port use	AFF A800		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e0b	e1b	9
	e0b	e1b	10
MetroCluster 2, MetroCluster interface	e0b	e1b	11
	e0b	e1b	12
MetroCluster 3, MetroCluster interface	e0b	e1b	13
	e0b	e1b	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling a AFF A900 to a Cisco 3232C or Cisco 9336C switch

Cabling an AFF A900 to a Cisco 3232C or Cisco 9336C-FX2 switch			
Port use	AFF A900		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface Ports for Transition (10/40/100Gbps)			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e5a	e7a	9
	e5a	e7a	10
MetroCluster 2, MetroCluster interface	e5a	e7a	11
	e5a	e7a	12
MetroCluster 3, MetroCluster interface	e5a	e7a	13
	e5a	e7a	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32
9336C-FX2 only: Ports disabled	9336C-FX2 only: Ports disabled		33
			34
			35
			36

Cabling an AFF A320, AFF A400, AFF A700 or AFF A800 to a Cisco 9336C-FX2 shared switch

Cabling an AFF A320, A400, A700, and A800 to a Cisco 9336C-FX2 shared switch			
MetroCluster 1, Local Cluster Interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster Interface			3
			4
Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b	5
	NSM-B, e0a	NSM-B, e0b	6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'	9
	Port 'A'	Port 'B'	10
MetroCluster 2, MetroCluster interface	Port 'A'	Port 'B'	11
	Port 'A'	Port 'B'	12
ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	ISL, MetroCluster	ISL, MetroCluster	13
			14
			15
			16
MetroCluster 1, Storage Interface	See Hardware Universe for available ports		17
			18
MetroCluster 2, Storage Interface			19
			20
Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b	21
	NSM-B, e0a	NSM-B, e0b	22
Storage shelf 3 (7)	NSM-A, e0a	NSM-A, e0b	23
	NSM-B, e0a	NSM-B, e0b	24
Storage shelf 4 (6)	NSM-A, e0a	NSM-A, e0b	25
	NSM-B, e0a	NSM-B, e0b	26
Storage shelf 5 (5)	NSM-A, e0a	NSM-A, e0b	27
	NSM-B, e0a	NSM-B, e0b	28
Storage shelf 6 (4)	NSM-A, e0a	NSM-A, e0b	29
	NSM-B, e0a	NSM-B, e0b	30
Storage shelf 7 (3)	NSM-A, e0a	NSM-A, e0b	31
	NSM-B, e0a	NSM-B, e0b	32
Storage shelf 8 (2)	NSM-A, e0a	NSM-A, e0b	33
	NSM-B, e0a	NSM-B, e0b	34
Storage shelf 9 (1)	NSM-A, e0a	NSM-A, e0b	35
	NSM-B, e0a	NSM-B, e0b	36

MetroCluster interfaces per platform		
Platform	Port 'A'	Port 'B'
AFF A320	e0g	e0h
AFF A400	e1a	e1b
AFF A700	e5a	e5b
AFF A800	e0b	e1b

Platform port assignments for Broadcom supported BES-53248 IP switches

The port usage in a MetroCluster IP configuration depends on the switch model and platform type.

The switches cannot be used with remote ISL ports of different speeds (for example, a 25 Gbps port connected to a 10 Gbps ISL port).

Notes for the tables below:

1. For some platforms, you can use ports 49 - 54 for MetroCluster ISLs or MetroCluster interface connections.

   These ports require an additional license.

2. Only a single four-node MetroCluster using A320 systems can be connected to the switch.

   Features that require a switched cluster are not supported in this configuration, including MetroCluster FC to IP transition and tech refresh procedures.

3. AFF A320 systems configured with Broadcom BES-53248 switches might not support all features.

   Any configuration or feature that requires that the local cluster connections are connected to a switch is not supported. For example, the following configurations and procedures are not supported:

   - Eight-node MetroCluster configurations
   - Transitioning from MetroCluster FC to MetroCluster IP configurations
   - Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Switch port usage for AFF A220 or FAS2750 systems

Cabling a AFF A220 or FAS2750 to a Broadcom BES-53248 switch			
Port use	FAS2750, A220		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1-6
MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	9
	e0a	e0b	10
MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b	11
	e0a	e0b	12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Switch port usage for AFF A250 or FAS500f systems

Cabling a AFF A250 or FAS500f to a Broadcom BES-53248 switch			
Port use	FAS500f, A250		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1-6
MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	9
	e0c	e0d	10
MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d	11
	e0c	e0d	12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Switch port usage for AFF A300 or FAS8200 systems

Cabling a AFF A300 or FAS8200 to a Broadcom BES-53248 switch			
Port use	FAS8200, AFF A300		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 1, MetroCluster interface	e1a	e1b	5
	e1a	e1b	6
MetroCluster 2, MetroCluster interface	e1a	e1b	7
	e1a	e1b	8
Unused	-		9
			10
			11
			12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Cabling a AFF A320 to a Broadcom BES-53248 switch			
Port use	AFF A320		Switch port
	IP_switch_x_1	IP_switch_x_2	
Ports not used	Ports not used		1 - 12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Ports not licensed (17 - 52)			..
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
MetroCluster 1, MetroCluster interface (see note 2)	e0g	e0h	55
	e0g	e0h	56

Switch port usage for AFF A400, FAS8300 or FAS8700 systems

Cabling a FAS8300, A400 or FAS8700 to a Broadcom BES-53248 switch			
Port use	FAS8300,FAS8700, A400		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1 - 12
ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 48
MetroCluster 5, Local Cluster interface (see note 1)	See Hardware Universe for available ports		49
			50
MetroCluster 5, MetroCluster interface (see note 1)	e1a	e1b	51
	e1a	e1b	52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Cabling the controller peering, data, and management ports

You must cable the controller module ports used for cluster peering, management and data connectivity.

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.

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

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

   Use the installation instructions for your platform at the AFF and FAS System Documentation.

Configure the MetroCluster IP switches

Configuring Broadcom IP switches

You must configure the Broadcom IP switches for use as the cluster interconnect and for backend MetroCluster IP connectivity.

Resetting the Broadcom IP switch to factory defaults

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

About this task

- You must repeat these steps on each of the IP switches in the MetroCluster IP configuration.
- You must be connected to the switch using the serial console.
- This task resets the configuration of the management network.

Steps

1. Change to the elevated command prompt (#): `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Erase the startup configuration and remove the banner
   a. Erase the startup configuration:

      `erase startup-config`

```
(IP_switch_A_1) #erase startup-config

Are you sure you want to clear the configuration? (y/n) y

(IP_switch_A_1) #
```

      This command does not erase the banner.

   b. Remove the banner:

      `no set clibanner`

```
(IP_switch_A_1) #configure
(IP_switch_A_1)(Config) # no set clibanner
(IP_switch_A_1)(Config) #
```

3. Reboot the switch: **`(IP_switch_A_1) #reload`**

```
Are you sure you would like to reset the system? (y/n) y
```

> If the system asks whether to save the unsaved or changed configuration before reloading the switch, select **No**.

4. Wait for the switch to reload, and then log in to the switch.

   The default user is “admin”, and no password is set. A prompt similar to the following is displayed:

   ```
   (Routing)>
   ```

5. Change to the elevated command prompt:

   `enable`

   ```
   Routing)> enable
   (Routing) #
   ```

6. Set the service port protocol to `none`:

   `serviceport protocol none`

   ```
   (Routing) #serviceport protocol none
   Changing protocol mode will reset ip configuration.
   Are you sure you want to continue? (y/n) y

   (Routing) #
   ```

7. Assign the IP address to the service port:

   `serviceport ip` *`ip-address netmask gateway`*

   The following example shows a service port assigned IP address "10.10.10.10" with subnet "255.255.255.0" and gateway "10.10.10.1":

   ```
   (Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
   ```

8. Verify that the service port is correctly configured:

   `show serviceport`

   The following example shows that the port is up and the correct addresses have been assigned:

```
(Routing) #show serviceport

Interface Status.............................. Up
IP Address..................................... 10.10.10.10
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.10.10.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:56:87:D7

(Routing) #
```

9. If desired, configure the SSH server.

   The RCF file disables the Telnet protocol. If you do not configure the SSH server, you can only access the bridge using the serial port connection.

   a. Generate RSA keys.

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate rsa
   ```

   b. Generate DSA keys (optional)

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate dsa
   ```

   c. If you are using the FIPS compliant version of EFOS, generate the ECDSA keys. The following example creates the keys with a length of 256. Valid values are 256, 384 or 521.

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate ecdsa 256
   ```

   d. Enable the SSH server.

   If necessary, exit the configuration context.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

If keys already exist, then you might be asked to overwrite them.

10. If desired, configure the domain and name server:

    `configure`

    The following example shows the `ip domain` and `ip name server` commands:

    ```
    (Routing) # configure
    (Routing) (Config)#ip domain name lab.netapp.com
    (Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
    (Routing) (Config)#exit
    (Routing) (Config)#
    ```

11. If desired, configure the time zone and time synchronization (SNTP).

    The following example shows the `sntp` commands, specifying the IP address of the SNTP server and the relative time zone.

    ```
    (Routing) #
    (Routing) (Config)#sntp client mode unicast
    (Routing) (Config)#sntp server 10.99.99.5
    (Routing) (Config)#clock timezone -7
    (Routing) (Config)#exit
    (Routing) (Config)#
    ```

12. Configure the switch name:

    `hostname IP_switch_A_1`

    The switch prompt will display the new name:

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Save the configuration:

    `write memory`

    You receive prompts and output similar to the following example:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

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

Downloading and installing the Broadcom switch EFOS software

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

About this task

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

Note the following:

- When upgrading from EFOS 3.4.x.x to EFOS 3.7.x.x or later, the switch must be running EFOS 3.4.4.6 (or later 3.4.x.x release). If you are running a release prior to that, then upgrade the switch to EFOS 3.4.4.6 (or later 3.4.x.x release) first, then upgrade the switch to EFOS 3.7.x.x or later.
- The configuration for EFOS 3.4.x.x and 3.7.x.x or later are different. Changing the EFOS version from 3.4.x.x to 3.7.x.x or later, or vice versa, requires the switch to be reset to factory defaults and the RCF files for the corresponding EFOS version to be (re)applied. This procedure requires access through the serial console port.
- Beginning with EFOS version 3.7.x.x or later, a non-FIPS compliant and a FIPS compliant version is available. Different steps apply when moving to from a non-FIPS compliant to a FIPS compliant version or vice versa. Changing EFOS from a non-FIPS compliant to a FIPS compliant version or vice versa will reset the switch to factory defaults. This procedure requires access through the serial console port.

Procedure	Current EFOS version	New EFOS version	High level steps

Steps to upgrade EFOS between two (non) FIPS compliant versions	3.4.x.x	3.4.x.x	Install the new EFOS image using method 1) The configuration and license information is retained
	3.4.4.6 (or later 3.4.x.x)	3.7.x.x or later non-FIPS compliant	Upgrade EFOS using method 1. Reset the switch to factory defaults and apply the RCF file for EFOS 3.7.x.x or later
	3.7.x.x or later non-FIPS compliant	3.4.4.6 (or later 3.4.x.x)	Downgrade EFOS using method 1. Reset the switch to factory defaults and apply the RCF file for EFOS 3.4.x.x
		3.7.x.x or later non-FIPS compliant	Install the new EFOS image using method 1. The configuration and license information is retained
	3.7.x.x or later FIPS compliant	3.7.x.x or later FIPS compliant	Install the new EFOS image using method 1. The configuration and license information is retained
Steps to upgrade to/from a FIPS compliant EFOS version	Non-FIPS compliant	FIPS compliant	Installation of the EFOS image using method 2. The switch configuration and license information will be lost.
	FIPS compliant	Non-FIPS compliant	

- Method 1: Steps to upgrade EFOS with downloading the software image to the backup boot partition
- Method 2: Steps to upgrade EFOS using the ONIE OS installation

Steps to upgrade EFOS with downloading the software image to the backup boot partition

You can perform the following steps only if both EFOS versions are non-FIPS compliant or both EFOS versions are FIPS compliant.

Do not use these steps if one version is FIPS compliant and the other version is non-FIPS compliant.

Steps

1. Copy the switch software to the switch: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

In this example, the efos-3.4.4.6.stk operating system file is copied from the SFTP server at 50.50.50.50 to the backup partition. You need to 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://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /switchsoftware/
Filename..................................... efos-3.4.4.6.stk
Data Type.................................... Code
Destination Filename......................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Set the switch to boot from the backup partition on the next switch reboot:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Verify that the new boot image will be active on the next boot:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Save the configuration:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Reboot the switch:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Wait for the switch to reboot.

In rare scenarios the switch may fail to boot. Follow the Steps to upgrade EFOS using the ONIE OS installation to install the new image.

7. If you change the switch from EFOS 3.4.x.x to EFOS 3.7.x.x or vice versa then follow the following two procedures to apply the correct configuration (RCF):
   a. Resetting the Broadcom IP switch to factory defaults
   b. Downloading and installing the Broadcom RCF files
8. Repeat these steps on the remaining three IP switches in the MetroCluster IP configuration.

Steps to upgrade EFOS using the ONIE OS installation

You can perform the following steps if one EFOS version is FIPS compliant and the other EFOS version is non-FIPS compliant. These steps can be used to install the non-FIPS or FIPS compliant EFOS 3.7.x.x image from ONIE if the switch fails to boot.

Steps

1. Boot the switch into ONIE installation mode.

   During boot, select ONIE when the following screen appears:

```
+----------------------------------------------------------------------+
|EFOS                                                                  |
|*ONIE                                                                 |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
+----------------------------------------------------------------------+
```

   After selecting "ONIE", the switch will then load and present you with the following choices:

```
 +------------------------------------------------------------------------+
 |*ONIE: Install OS                                                       |
 | ONIE: Rescue                                                           |
 | ONIE: Uninstall OS                                                     |
 | ONIE: Update ONIE                                                      |
 | ONIE: Embed ONIE                                                       |
 | DIAG: Diagnostic Mode                                                  |
 | DIAG: Burn-In Mode                                                     |
 |                                                                        |
 |                                                                        |
 |                                                                        |
 |                                                                        |
 |                                                                        |
 +------------------------------------------------------------------------+
```

The switch now will boot into ONIE installation mode.

2. Stop the ONIE discovery and configure the ethernet interface

   Once the following message appears press <enter> to invoke the ONIE console:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   The ONIE discovery will continue and messages will be printed to the console.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Configure the ethernet interface and add the route using `ifconfig eth0 <ipAddress> netmask <netmask> up` and `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Verify that the server hosting the ONIE installation file is reachable:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Install the new switch software

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

The software will install and then reboot the switch. Let the switch reboot normally into the new EFOS version.

6. Verify that the new switch software is installed

`show bootvar`

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Complete the installation

   The switch will reboot with no configuration applied and reset to factory defaults. Follow the two procedures to configure the switch basic settings and apply the RCF file as outlined in the following two documents:

   a. Configure the switch basic settings. Follow step 4 and later: Resetting the Broadcom IP switch to factory defaults
   b. Create and apply the RCF file as outlined in Downloading and installing the Broadcom RCF files

Downloading and installing the Broadcom RCF files

You must download and install the switch RCF file to each switch in the MetroCluster IP configuration.

Before you begin

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

About this task

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

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

Switch	RCF file
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_A_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt

The RCF files for EFOS version 3.4.4.6 or later 3.4.x.x. release and EFOS version 3.7.0.4 are different. You need to make sure that you have created the correct RCF files for the EFOS version that the switch is running.

EFOS version	RCF file version
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Steps

1. Generate the Broadcom RCF files for MetroCluster IP.
   a. Download the RcfFileGenerator for MetroCluster IP
   b. Generate the RCF file for your configuration using the RcfFileGenerator for MetroCluster IP
2. Copy the RCF files to the switches:
   a. Copy the RCF files to the first switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF nvram:script BES-53248_v1.32_Switch-`

```
A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr
```

In this example, the "BES-53248_v1.32_Switch-A1.txt" RCF file is copied from the SFTP server at "50.50.50.50" to the local bootflash. You need to 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://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /RcfFiles/
Filename..................................... BES-
53248_v1.32_Switch-A1.txt
Data Type.................................... Config Script
Destination Filename......................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"************************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248


...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Verify that the RCF file is saved as a script:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr            852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Apply the RCF script:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"*****************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Save the configuration:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Reboot the switch:

`reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

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

3. Reload the switch:

`reload`

```
IP_switch_A_1# reload
```

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

Configure Cisco IP switches

Configuring Cisco IP switches

You must configure the Cisco IP switches for use as the cluster interconnect and for backend MetroCluster IP connectivity.

About this task

- You must repeat these steps on each of the IP switches in the MetroCluster IP configuration.
- You must be connected to the switch using the serial console.
- This task resets the configuration of the management network.

Resetting the Cisco IP switch to factory defaults

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

About this task

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

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 (RSA) 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 configuring 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.
```

You enter basic information in the next set of prompts, including the switch name, management address, and gateway, and select SSH with RSA.

```
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 prompts 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 IP configuration.

Downloading and installing the Cisco switch NX-OS software

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

About this task

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 IP switches in the MetroCluster IP configuration.

You must use the supported switch software version.

NetApp Hardware Universe

Steps

1. Download the supported NX-OS software file.

   Cisco Software Download

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 nxos bootflash:nxos.version-number.bin`

   The switch will reload (reboot) automatically after the switch software has been installed.

   The following example shows the software installation on IP_switch_A_1:

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

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

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

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

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

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos               7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

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 IP switches in the MetroCluster IP configuration.

Downloading and installing the Cisco IP RCF files

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

About this task

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 IP switches in the MetroCluster IP 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 IP configuration. You must use the correct RCF files for the switch model you are using.

Switch	RCF file
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

Steps

1. Download the MetroCluster IP 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_v1.80_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. Configure the TCAM regions on Cisco 3132Q-V and Cisco 3232C switches.

   Skip this step if you do not have Cisco 3132Q-V or Cisco 3232C switches.

   a. On Cisco 3132Q-V switch, set the following TCAM regions:

      ```
      conf t
      hardware access-list tcam region span 0
      hardware access-list tcam region racl 256
      hardware access-list tcam region e-racl 256
      hardware access-list tcam region qos 256
      ```

   b. On Cisco 3232C switch, set the following TCAM regions:

      ```
      conf t
      hardware access-list tcam region span 0
      hardware access-list tcam region racl-lite 0
      hardware access-list tcam region racl 256
      hardware access-list tcam region e-racl 256
      hardware access-list tcam region qos 256
      ```

c. After setting the TCAM regions, save the configuration and reload the switch:

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

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

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

6. 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
```

7. Reload the switch:

```
reload
```

```
IP_switch_A_1# reload
```

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

Configuring MACsec encryption on Cisco 9336C switches

You must only configure MACsec encryption on the WAN ISL ports that run between the sites. You must configure MACsec after applying the correct RCF file.

Licensing requirements for MACsec

MACsec requires a security license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply for licenses, see the Cisco NX-OS Licensing Guide

Enabling Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You can enable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

Steps

1. Enter the global configuration mode:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Enable MACsec and MKA on the device:

   `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copy the running configuration to the startup configuration:

   `copy running-config startup-config`

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

Disabling Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You might need to disable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

Steps

1. Enter the global configuration mode:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disable the MACsec configuration on the device:

   `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

   Selecting the “no” option restores the MACsec feature.

3. Select the interface that you already configured with MACsec.

   You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Remove the keychain, policy and fallback-keychain configured on the interface to remove the MACsec configuration:

   ```
   no macsec keychain keychain-name policy policy-name fallback-keychain
   keychain-name
   ```

   ```
   IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
   keychain fb_kc2
   ```

5. Repeat steps 3 and 4 on all interfaces where MACsec is configured.
6. Copy the running configuration to the startup configuration:

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

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

Configuring a MACsec key chain and keys

You can create a MACsec key chain or keys on your configuration.

Key Lifetime and Hitless Key Rollover

A MACsec keychain can have multiple pre-shared keys (PSKs), each configured with a key ID and an optional lifetime. A key lifetime specifies at which time the key activates and expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared key in the keychain after the lifetime is expired. The time zone of the key can be local or UTC. The default time zone is UTC. A key can roll over to a second key within the same keychain if you configure the second key (in the keychain) and configure a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless (that is, the key rolls over without traffic interruption).

Fallback Key

A MACsec session can fail due to a key/key name (CKN) mismatch or a finite key duration between the switch and a peer. If a MACsec session does fail, a fallback session can take over if a fallback key is configured. A fallback session prevents downtime due to primary session failure and allows a user time to fix the key issue causing the failure. A fallback key also provides a backup session if the primary session fails to start. This feature is optional.

Steps

1. Enter the global configuration mode:

   ```
   configure terminal
   ```

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. To hide the encrypted key octet string, replace the string with a wildcard character in the output of the `show running-config` and `show startup-config` commands:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

NOTE:

The octet string is also hidden when you save the configuration to a file.

By default, PSK keys are displayed in encrypted format and can easily be decrypted. This command applies only to MACsec key chains.

3. Create a MACsec key chain to hold a set of MACsec keys and enter MACsec key chain configuration mode:

`key chain name macsec`

```
IP_switch_A_1(config)# key chain 1 macsec
IP_switch_A_1(config-macseckeychain)#
```

4. Create a MACsec key and enter MACsec key configuration mode:

`key key-id`

The range is from 1 to 32 hex digit key-string, and the maximum size is 64 characters.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configure the octet string for the key:

`key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```

> The octet-string argument can contain up to 64 hexadecimal characters. The octet key is encoded internally, so the key in clear text does not appear in the output of the `show running-config macsec` command.

6. Configure a send lifetime for the key (in seconds):

`send-lifetime start-time duration duration`

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

By default, the device treats the start time as UTC. The start-time argument is the time of day and date that the key becomes active. The duration argument is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).

7. Copy the running configuration to the startup configuration:

   `copy running-config startup-config`

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

8. Displays the keychain configuration:

   `show keychain name`

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configuring a MACsec policy

Steps

1. Enter the global configuration mode:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Create a MACsec policy:

   `macsec policy name`

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. Configure one of the following ciphers, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, or GCM-AES-XPN-256:

   `cipher-suite name`

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configure the key server priority to break the tie between peers during a key exchange:

   `key-server-priority number`

   ```
   switch(config-macsec-policy)# key-server-priority 0
   ```

5. Configure the security policy to define the handling of data and control packets:

   `security-policy security policy`

   Choose a security policy from the following options:

   - must-secure — packets not carrying MACsec headers are dropped
   - should-secure — packets not carrying MACsec headers are permitted (this is the default value)

   ```
   IP_switch_A_1(config-macsec-policy)# security-policy should-secure
   ```

6. Configure the replay protection window so the secured interface does not accept a packet that is less than the configured window size: `window-size number`

   > The replay protection window size represents the maximum out-of-sequence frames that MACsec accepts and are not discarded. The range is from 0 to 596000000.

   ```
   IP_switch_A_1(config-macsec-policy)# window-size 512
   ```

7. Configure the time in seconds to force an SAK rekey:

   `sak-expiry-time time`

   You can use this command to change the session key to a predictable time interval. The default is 0.

   ```
   IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
   ```

8. Configure one of the following confidentiality offsets in the layer 2 frame where encryption begins:

   `conf-offsetconfidentiality offset`

   Choose from the following options:

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

   ```
   IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
   ```

This command might be necessary for intermediate switches to use packet headers (dmac, smac, etype) like MPLS tags.

9. Copy the running configuration to the startup configuration:

   `copy running-config startup-config`

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

10. Display the MACsec policy configuration:

    `show macsec policy`

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

Verifying the MACsec configuration

Steps

1. Repeat **all** of the previous procedures on the second switch within the configuration to establish a MACsec session.
2. Run the following commands to verify that both switches are successfully encrypted:
   a. Run: `show macsec mka summary`
   b. Run: `show macsec mka session`
   c. Run: `show macsec mka statistics`

   You can verify the MACsec configuration using the following commands:

Command	Displays information about…
`show macsec mka session interface typeslot/port number`	The MACsec MKA session for a specific interface or for all interfaces
`show key chain name`	The key chain configuration
`show macsec mka summary`	The MACsec MKA configuration
`show macsec policy policy-name`	The configuration for a specific MACsec policy or for all MACsec policies

Configuring a MACsec fallback key on a WAN ISL port

You can configure a fallback key to initiate a backup session if the primary session fails as a result of a key/key name (CKN) mismatch or a finite key duration between the switch and peer.

Steps

1. Enter the global configuration mode:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Specify the interface that you are configuring.

   You can specify the interface type and identity. For an Ethernet port, use:

   `ethernet slot/port`

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

3. Specify the fallback key chain for use after a MACsec session failure due to a key/key ID mismatch or a key expiration:

   `macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

   > You should configure the fallback-keychain using the steps in *Configuring a MACsec key chain and keys* before proceeding with this step.

   ```
   IP_switch_A_1(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2
   ```

4. Repeat the previous steps to configure additional WAN ISL ports with MACsec.
5. Copy the running configuration to the startup configuration:

   `copy running-config startup-config`

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

Setting Forward Error Correction for systems using 25-Gbps connectivity

If your system is configured using 25-Gbps connectivity, you need to set the Forward Error Correction (fec) parameter manually to off after applying the RCF file. The RCF file does not apply this setting.

About this task

The 25-Gbps ports must be cabled prior to performing this procedure.

Platform port assignments for Cisco 3232C or Cisco 9336C switches

This task only applies to platforms using 25-Gbps connectivity: • AFF A300 • FAS 8200 • FAS 500f • AFF A250

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

Steps

1. Set the `fec` parameter to “off” on each 25-Gbps port that is connected to a controller module, and then copy the running configuration to the startup configuration:
   a. Enter configuration mode:

      ```
      config t
      ```

   b. Specify the 25-Gbps interface to configure:

      ```
      interface interface-ID
      ```

   c. Set `fec` to “off”:

      ```
      fec off
      ```

   d. Repeat the previous steps for each 25-Gbps port on the switch.
   e. Exit configuration mode:

      ```
      exit
      ```

      The following example shows the commands for interface Ethernet1/25/1 on switch IP_switch_A_1:

      ```
      IP_switch_A_1# conf t
      IP_switch_A_1(config)# interface Ethernet1/25/1
      IP_switch_A_1(config-if)# fec off
      IP_switch_A_1(config-if)# exit
      IP_switch_A_1(config-if)# end
      IP_switch_A_1# copy running-config startup-config
      ```

2. Repeat the previous step on the other three switches in the MetroCluster IP configuration.

Configuring MACsec encryption on Cisco 9336C switches

If desired, you can configure MACsec encryption on the WAN ISL ports that run between the sites. You must configure MACsec after applying the correct RCF file.

MACsec encryption can only be applied to the WAN ISL ports.

Licensing requirements for MACsec

MACsec requires a security license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply for licenses, see the Cisco NX-OS Licensing Guide

Enabling Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You can enable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP

configuration.

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Enable MACsec and MKA on the device: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

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

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

Disabling Cisco MACsec Encryption

You might need to disable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

If you disable encryption, you must also delete your keys, as described in XXX.

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disable the MACsec configuration on the device: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

Selecting the no option restores the MACsec feature.

3. Select the interface that you already configured with MACsec.

   You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Remove the keychain, policy and fallback-keychain configured on the interface to remove the MACsec

configuration: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Repeat steps 3 and 4 on all interfaces where MACsec is configured.
6. Copy the running configuration to the startup configuration: `copy running-config startup-config`

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

Configuring a MACsec key chain and keys

For details on configuring a MACsec key chain, see the Cisco documentation for your switch.