

AFF and FAS Switch Documentation

ONTAP Systems Switches

NetApp April 08, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems-switches/index.html on April 08, 2022. Always check docs.netapp.com for the latest.

Table of Contents

AFF and FAS Switch Documentation	1
Broadcom-supported BES-53248 switches	2
Overview of the Broadcom-supported BES-53248 cluster switch	2
Set up the switch	3
Migrate from CN1610 switches to BES-53248 switches	40
Migrate to a two-node switched cluster	57
Upgrade a switch in an NDO/NDU environment	71
Replace a Broadcom-supported BES-53248 cluster switch - BES-53248 switches	. 112
Cisco Nexus 3132Q-V switches	. 124
Cisco Nexus 3132Q-V switches	. 124
Install a Cisco Nexus 3132Q-V cluster switch and a pass-through panel in a NetApp cabinet	. 125
Set up	. 129
Install NX-OS software and RCFs on Cisco Nexus 3132Q-V cluster switches	. 157
Migrate to a two-node switched cluster with Cisco Nexus 3132Q-V cluster switches	. 184
Replace Cisco Nexus 3132Q-V cluster switches	. 204
Replace a Cisco Nexus 5596 cluster switch with a Cisco Nexus 3132Q-V cluster switch	. 228
Replace CN1610 cluster switches with Cisco Nexus 3132Q-V cluster switches	. 257
Cisco Nexus 3232C switches	. 286
Cisco Nexus 3232C switches	. 286
Install a Cisco Nexus 3232C cluster switch and a pass-through panel in a NetApp cabinet	. 287
Set up	. 291
Install NX-OS software and RCFs on Cisco Nexus 3232C cluster switches	. 319
Migrate a CN1610 switch to a Cisco Nexus 3232C cluster switch	. 348
Migrate from a Cisco Nexus 5596 switch to a Cisco Nexus 3232C switch	. 376
Migrate from a two-node switchless cluster to a cluster with Cisco Nexus 3232C cluster switches	. 404
Replace a Cisco Nexus 3232C cluster switch	. 421
Replace a Cisco Nexus 3232C storage switch	. 444
Upgrade a Cisco Nexus 3232C storage switch	. 449
Cisco Nexus 9336C-FX2 switches	. 459
Cisco 9336C-FX2 switch overview.	. 459
Install a Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet	. 460
Set up	. 464
Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 cluster switches	. 492
Migrate from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch	. 521
Migrate to a two-node switched cluster with Cisco Nexus 9336C-FX2 cluster switches	. 538
Configure a Cisco Nexus 9336C-FX2 cluster switch	. 551
Replace a Cisco Nexus 9336C-FX2 cluster switch	. 580
Replace a Cisco Nexus 9336C-FX2 storage switch	. 594
Cisco 9336C-FX2 shared switch overview	. 600
Setup and configuration guide for Cisco shared switches	. 600
Install NX-OS software and RCFs	. 608
Migrate from a switchless cluster with direct-attached storage by adding two new shared switches	. 647
Migrate from a switched configuration with direct-attached storage by adding two new shared switches	. 663

Migrate from a switchless configuration with switch-attached storage by reusing the storage switches 6	368
Migrate from a switched cluster with switch-attached storage by reusing the storage switches	372
Replace a Cisco Nexus 9336C-FX2 shared switch	377
Cisco Nexus 92300YC switches	392
Cisco Nexus 92300YC switch overview 6	392
Set up	393
Configure a new Cisco Nexus 92300YC switch	722
Install NX-OS software and RCF on Cisco Nexus 92300YC cluster switches	737
Migrate to a two-node switched cluster with Cisco Nexus 92300YC switches	754
Migrate from a Cisco switch to a Cisco Nexus 92300YC switch	767
NetApp CN1610 switches	798
NetApp CN1610 Switches	798
Install FASTPATH software and RCFs on a NetApp cluster switch	798
Install FASTPATH software and RCFs on NetApp cluster switches running ONTAP 8.3.1 and later 8	313
Migrate to a two-node switched cluster with NetApp CN1610 cluster switches	325
Migrate from a switchless cluster environment to a switched NetApp CN1610 cluster environment 8	325
Migrate to a two-node switched cluster in FAS22xx systems with a single cluster-network connection 8	344
CN1601 and CN1610 Switch Setup and Configuration	348
CN1610 Network Switch CLI Command Reference - Version 1.2.x.x	348
CN1610 Network Switch CLI Command Reference - Version 1.2.x.x	348
NetApp 10G Cluster-Mode Switch Installation	348
NetApp CN1610 Switch Administrator's Guide - Version 1.1.x.x	348
NetApp CN1610 Switch Administrator's Guide - Version 1.2.x.x	348
CN1601 Network Switch CLI Command Reference	348
CN1601 Switch Administrator	349
NetApp 1G Cluster-Mode Switch Installation	349
NVIDIA MSN2100 Switches	350
Other switch models	351
Other Cisco Cluster, Storage and Management Switches	351
Legal notices	852
Copyright	852
Trademarks	852
Patents	852
Privacy policy	852
Open source	352

AFF and FAS Switch Documentation

Broadcom-supported BES-53248 switches

Overview of the Broadcom-supported BES-53248 cluster switch

Broadcom-supported BES-53248 cluster switches are designed to work in clusters ranging in size from two to 24 nodes in ONTAP 9.5P8 and later. Support for 40/100 GbE cluster ports starts with EFOS firmware version 3.4.4.6 and later.

BES-53248 is a switch running on a Broadcom-embedded OS known as Ethernet Fabric OS (EFOS).

The following table lists the part number and description for the BES-53248 cluster switch, rack mount rail kit, fans, and power supplies:

Part number	Description
X190005	BES-53248, CLSW, 16Pt10/25GB, PTSX, BRDCM SUPP (PTSX = Port Side Exhaust)
X190005R	BES-53248, CLSW, 16Pt10/25GB, PSIN, BRDCM SUPP (PSIN = Port Side Intake)
X-RAIL-4POST-190005	Rack mount rail kit Ozeki 4 post 19"
X-FAN-190005-R	Fan, port side intake X190005
X-FAN-190005-F	Fan, port side exhaust X190005
X-PSU-190005-R	Power supply, port side intake X190005
X-PSU-190005-F	Power supply, port side exhaust X190005

Overview of airflow based on the two models offered:

- Port-side exhaust airflow (standard air): Cool air enters the chassis through the fan and power supply modules in the cold aisle and exhausts through the port end of the chassis in the hot aisle. Blue coloring indicates port-side exhaust airflow. This is the most common option.
- Port-side intake airflow (reverse air): Cool air enters the chassis through the port end in the cold aisle and exhausts through the fan and power supply modules in the hot aisle.

See the NetApp KB article: How to add additional port licensing for the Broadcom-supported BES-53248 switch for details on adding additional port licenses.

For information on the relevant connectors and cable options to use along with their part numbers, see the NetApp Hardware Universe.

For more information, see the *Cluster Network and Management Network Compatibility Matrix* available from the BES-53248 switch download site Broadcom cluster switches.

Set up the switch

BES-53248 cluster switch required documentation

You need specific switch and controller documentation to set up your Cluster-Mode configuration.

Required documentation for BES-53248 cluster switches

To set up the BES-53248 cluster switch, you need the following documents available from the Broadcom Support Site: Broadcom Ethernet Switch Product Line

Document title	Description
EFOS Administrator's Guide v3.4.3	Provides examples of how to use the BES-53248 switch in a typical network.
EFOS CLI Command Reference v3.4.3	Describes the command-line interface (CLI) commands you use to view and configure the BES-53248 software.
EFOS Getting Started Guide v3.4.3	Provides detailed information about for the BES-53248 switch.
EFOS SNMP Reference Guide v3.4.3	Provides examples of how to use the BES-53248 switch in a typical network.
EFOS Scaling Parameters and Values v3.4.3	Describes the default scaling parameters with which EFOS software is delivered and validated on the supported platforms.
EFOS Functional Specifications v3.4.3	Describes the specifications for the EFOS software on the supported platforms.
EFOS Release Notes v3.4.3	Provides release-specific information about BES-53248 software.

Required documentation for supported ONTAP systems

To set up an ONTAP system, you need the following documents from the NetApp Support Site at mysupport.netapp.com

Name	Description
Hardware Universe	Describes the power and site requirements for all NetApp hardware, including system cabinets.
Controller-specific Installation and Setup Instructions	Describes how to install NetApp hardware.
ONTAP 9	Provides detailed information about all aspects of the ONTAP 9 release.

BES-53248 cluster switch configuration requirements

To configure your cluster, you need the appropriate number and type of cables and cable connectors for your cluster switches. Depending on the type of cluster switch you are initially configuring, you need to connect to the switch console port with the included console cable and you need specific network information.

Configure a new BES-53248 cluster switch

You can configure a new BES-53248 cluster switch by completing the steps detailed in this chapter.

About this task

Installing the BES-53248 cluster switch on systems running ONTAP starts with setting up an IP address and configuration to allow the switch to communicate through the management interface. Then you can install the Ethernet Fabric OS (EFOS) software, reference configuration file (RCF), and other licenses as needed. This procedure is intended for preparing the BES-53248 switch before controllers are added. In addition, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for the BES-53248 cluster switches. See Installing the Cluster Switch Health Monitor (CSHM) configuration file for more details.

The examples in this procedure use the following switch and node nomenclature:

- The NetApp switch names are cs1 and cs2.
- The example used in this procedure starts the upgrade on the second switch, cs2.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The IPspace name is Cluster.
- The cluster1::> prompt indicates the name of the cluster.
- The cluster ports on each node are named e0a and e0b.

See the NetApp Hardware Universe for the actual cluster ports supported on your platform.

- The Inter-Switch Links (ISLs) supported for the NetApp switches are ports 0/55 and 0/56.
- The node connections supported for the NetApp switches are ports 0/1 through 0/16 with default licensing.
- The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.

Initial installation of the BES-53248 cluster switch - BES-53248 switches

You can use this procedure to perform the initial installation of the BES-53248 cluster switch.

You can download the applicable Broadcom EFOS software for your cluster switches from the Broadcom Ethernet Switch Support site.

EFOS is a wide-ranging software set of advanced networking features and protocols necessary to develop a variety of Ethernet and IP infrastructure systems for data center applications. EFOS software is an architecture suitable for any network organizational device using leading-edge applications that require thorough packet inspection or separation.

This procedure provides a summary of the process to install your switches and get them running:

Steps

- 1. Connect the serial port to the host or serial port of your choice.
- 2. Connect the management port (the RJ-45 wrench port on the left side of the switch) to the same network where your TFTP server is located.
- 3. At the console, set the host side serial settings:
 - 115200 baud
 - 8 data bits
 - 1 stop bit
 - o parity: none
 - · flow control: none
- 4. Log in to the switch as admin and press enter when prompted for a password. The default switch name is routing. At the prompt, enable. This gives you access to Privileged EXEC mode for switch configuration.

```
User: admin
Password:
(Routing) > enable
Password:
(Routing) #
```

5. Change the switch name to cs2:

```
(Routing) # hostname cs2 (cs2) #
```

6. To set a static IP address, use the serviceport protocol, network protocol, and serviceport ip commands as shown in the example.

The serviceport is set to use DHCP by default. The IP address, subnet mask, and default gateway address are assigned automatically.

```
(cs2) # serviceport protocol none
(cs2) # network protocol none
(cs2) # serviceport ip ipaddr netmask gateway
```

7. Verify the results using the command:

```
show serviceport
```

The following example shows IP information provided by DHCP server.

8. Configure the domain and name server:

configure

```
(cs2) # configure
(cs2) (Config) # ip domain name company.com
(cs2) (Config) # ip name server 10.10.99.1 10.10.99.2
(cs2) (Config) # exit
(cs2) (Config) #
```

- 9. Configure the NTP server.
 - a. Configure the time zone and time synchronization (SNTP):

sntp

```
(cs2) #
(cs2) (Config) #sntp client mode unicast
(cs2) (Config) #sntp server 10.99.99.5
(cs2) (Config) #clock timezone -7
(cs2) (Config) #exit
(cs2) (Config) #
```

b. Configure the time manually:

clock

```
(cs2) #config
(cs2) (Config) #no sntp client mode
(cs2) (Config) #clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2) (Config) #clock timezone -5 zone EST
(cs2) (Config) #clock set 07:00:00
(cs2) (Config) #clock set 10/20/2020
(cs2) (Config) #show clock
07:00:11 EST(UTC-5:00) Oct 20 2020
No time source
(cs2) (Config) #exit
(cs2) #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!
```

Enable SSH on BES-53248 cluster switches - BES-53248 switches

SSH is a requirement when using the Cluster Switch Health Monitor (CSHM) and log collection features. To enable SSH on BES-53248 cluster switches, you generate the SSH keys first and then enable SSH.

Steps

1. Generate the SSH keys:

crypto key generate

```
(switch) # show ip ssh
SSH Configuration
Administrative Mode: ..... Disabled
SSH Port: ...... 22
Protocol Level: ...... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA (521)
Key Generation In Progress: ..... None
SCP server Administrative Mode: ..... Disabled
(switch) # config
(switch) (Config) # crypto key generate rsa
Do you want to overwrite the existing RSA keys? (y/n): y
(switch) (Config) # crypto key generate dsa
Do you want to overwrite the existing DSA keys? (y/n): y
(switch) (Config) # crypto key generate ecdsa 521
Do you want to overwrite the existing ECDSA keys? (y/n): y
(switch) (Config) # exit
```

2. Verify that SSH is enabled:

show ip ssh

```
(switch) # show ip sshSSH ConfigurationEnabledAdministrative Mode:EnabledSSH Port:22Protocol Level:Version 2SSH Sessions Currently Active:0Max SSH Sessions Allowed:5SSH Timeout (mins):5Keys Present:DSA(1024) RSA(1024)ECDSA(521)Key Generation In Progress:NoneSCP server Administrative Mode:Disabled(switch) #
```

Install the EFOS software

You can use this procedure to install the EFOS software on the BES-53248 cluster switch. You can download the applicable Broadcom EFOS software for your cluster switches from the Broadcom Ethernet Switch Support site.

About this task

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.

Steps to upgrade EFOS between two (non) FIPS compliant versions Steps to upgrade to/from a FIPS compliant EFOS version	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	
	Non-FIPS compliant	FIPS compliant	Installation of the EFOS image using method 2. The switch configuration	
	FIPS compliant	Non-FIPS compliant	and license information will be lost.	



Note that after upgrading BES-53248 cluster switches from EFOS 3.3.x.x or 3.4.x.x to EFOS 3.7.0.4 or 3.8.0.2, Inter-Switch Links (ISLs) and port channel are marked in the **Down** state. See this KB article for further details.

Steps

- 1. Connect the BES-53248 cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF file.

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Back up the current active image on cs2:

show bootvar

(cs2) # show bootvar Image Descriptions active : backup : Images currently available on Flash ______ unit active backup current-active next-active 1 3.4.3.3 Q.10.22.1 3.4.3.3 3.4.3.3 (cs2) # copy active backup Copying active to backup Management access will be blocked for the duration of the operation Copy operation successful (cs2) # show bootvar Image Descriptions active : backup : Images currently available on Flash _____ active backup current-active next-active 1 3.4.3.3 3.4.3.3 3.4.3.3 3.4.3.3 (cs2) #

4. Verify the running version of the EFOS software:

show version

(cs2) # show version
Switch: 1
System Description. Quanta IX8-B 48x25GB SFP 8x100GB QSFP, 3.4.3.3, Linux 4.4.117-ceeeb99d, 2016.05.00.04 Machine Type. Quanta IX8-B 48x25GB SFP 8x100GB QSFP Machine Model. IX8-B Serial Number. QTFCU38260014 Maintenance Level. A Manufacturer. 0xbc00 Burned In MAC Address. D8:C4:97:71:12:3D Software Version. 3.4.3.3 Operating System. Linux 4.4.117-ceeeb99d Network Processing Device. BCM56873_A0 CPLD Version. 0xff040c03
Additional Packages BGP-4 OOS Multicast IPv6 Routing Data Center OpEN API Prototype Open API

5. Download the image file to the switch.

Copying the image file to the active image means that when you reboot, that image establishes the running EFOS version. The previous image remains available as a backup.

6. Display the boot images for the active and backup configuration:

show bootvar

(cs2) # show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash

unit active backup current-active next-active

1 3.4.3.3 3.4.3.3 3.4.3.3 3.4.3.3 3.4.4.6

7. Reboot the switch:

reload

```
(cs2) # reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully .
Configuration Saved!
System will now restart!
```

8. Log in again and verify the new version of the EFOS software:

show version

```
(cs2) # show version
Switch: 1
System Description..... x86 64-
quanta common rglbmc-r0, 3.4.4.6, Linux 4.4.211-28a6fe76, 2016.05.00.04
Machine Type..... x86 64-
quanta common rglbmc-r0
Machine Model..... BES-53248
Maintenance Level..... A
Burned In MAC Address..... D8:C4:97:71:0F:40
Operating System..... Linux 4.4.211-28a6fe76
Network Processing Device..... BCM56873 A0
Additional Packages..... BGP-4
..... QOS
..... Multicast
..... IPv6
..... Routing
..... Data Center
 ..... Open Api
...... Prototype Open API
```

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.



This functionality is only available for EFOS 3.7.x.x or later non-FIPS compliant.

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:

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

7. Complete the installation.

The switch will reboot with no configuration applied and reset to factory defaults.

Related information

Broadcom Ethernet Switch Support

Install licenses

Install licenses for BES-53248 cluster switches - BES-53248 switches

The BES-53248 cluster switch base model is licensed for 16 10GbE or 25GbE ports and two 100GbE ports. New ports can be added by purchasing more licenses.

The following licenses are available for use on the BES-53248 cluster switch:

License type	License details
Supported firmware version	SW-BES-53248A1-G1-8P-LIC
Broadcom 8P 10-25,2P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES-53248A1-G1-16P-LIC	Broadcom 16P 10-25,4P40-100 License Key, X190005/R
EFOS 3.4.3.3 and later	SW-BES-53248A1-G1-24P-LIC
Broadcom 24P 10-25,6P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES54248-40-100G-LIC	Broadcom 6Port 40G100G License Key, X190005/R
EFOS 3.4.4.6 and later	SW-BES53248-8P-10G25G-LIC
Broadcom 8Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later
SW-BES53248-16P-1025G-LIC	Broadcom 16Port 10G25G License Key, X190005/R
EFOS 3.4.4.6 and later	SW-BES53248-24P-1025G-LIC
Broadcom 24Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF file.

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Check the current license usage on switch cs2:

show license

4. Install the license file. The following example uses SFTP to copy a license file to a key index 1.

Repeat this step to load more licenses and to use different key index numbers.

5. Display all current license information and note the license status before switch cs2 is rebooted:

show license

6. Display all licensed ports:

```
show port all | exclude Detach
```

The ports from the additional license files are not displayed until after the switch is rebooted.

		Admin	Physical	Physical	Link	Link	LACP
Actor		-	1	1			-
Intf	Туре	Mode	Mode	Status	Status	Trap	Mode
Timeout							
0/1		Disable	Auto		Down	Enable	Enable
long							
0/2		Disable	Auto		Down	Enable	Enable
long							
0/3		Disable	Auto		Down	Enable	Enable
long							
0/4		Disable	Auto		Down	Enable	Enable
long							
0/5		Disable	Auto		Down	Enable	Enable
long							
0/6		Disable	Auto		Down	Enable	Enable
long							
0/7		Disable	Auto		Down	Enable	Enable
long							
0/8		Disable	Auto		Down	Enable	Enable
long		D' 11			_	- 11	- 11
0/9		Disable	Auto		Down	Enable	Enable
long 0/10		Disable	711+0		Dorra	Enable	Enabla
long		DISABLE	Auto		Down	Eliable	Eliable
0/11		Disable	Δ11±0		Down	Enable	Enable
long		DISABIC	Auco		DOWII	Enable	HIRDIC
0/12		Disable	Auto		Down	Enable	Enable
long		2130210	11400		20111		LIIGNIC
0/13		Disable	Auto		Down	Enable	Enable
long							
0/14		Disable	Auto		Down	Enable	Enable
long							
0/15		Disable	Auto		Down	Enable	Enable
long							
0/16		Disable	Auto		Down	Enable	Enable
long							
0/55		Disable	Auto		Down	Enable	Enable
long							
0/56		Disable	Auto		Down	Enable	Enable
long							

7. Reboot the switch:

reload

```
(cs2) # reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully .
Configuration Saved!
Are you sure you would like to reset the system? (y/n) y
```

8. Check that the new license is active and note that the license has been applied:

show license

9. Check that all new ports are available:

show port all | exclude Detach

```
(cs2) # show port all \| exclude Detach

Admin Physical Physical Link Link LACP

Actor
Intf Type Mode Mode Status Status Trap Mode

Timeout

-----
0/1 Disable Auto Down Enable Enable
long
```

0/2	Disable	Auto	Down	Enable	Enable
long 0/3	Disable	Auto	Down	Enable	Enable
long	Disable	7	D	D l- l -	D., . l. l .
0/4 long	Disable	Auto	Down	Enable	Enable
0/5	Disable	Auto	Down	Enable	Enable
long 0/6	Disable	Auto	Down	Enable	Enable
long 0/7	Disable	A + - 0	Dorra	Enable	Enable
long	DISABle	Auto	Down	Ellable	Eliable
0/8 long	Disable	Auto	Down	Enable	Enable
0/9	Disable	Auto	Down	Enable	Enable
long 0/10	Disable	Auto	Down	Enable	Enable
long		11400	Down.		
0/11 long	Disable	Auto	Down	Enable	Enable
0/12	Disable	Auto	Down	Enable	Enable
long 0/13	Disable	Auto	Down	Enable	Enable
long					
0/14 long	Disable	Auto	Down	Enable	Enable
0/15	Disable	Auto	Down	Enable	Enable
long 0/16	Disable	Auto	Down	Enable	Enable
long	_, _,		_		
0/49 long	Disable	100G Full	Down	Enable	Enable
0/50	Disable	100G Full	Down	Enable	Enable
long 0/51	Disable	100G Full	Down	Enable	Enable
long	Disable	1000 5-11	D	D l- l -	D., . l. l .
0/52 long	Disable	100G Full	Down	Enable	Enable
0/53	Disable	100G Full	Down	Enable	Enable
long 0/54	Disable	100G Full	Down	Enable	Enable
long 0/55	Disable	100G Full	Down	Enable	Enable
long	DISABLE	TOOG FULL	DOWII	Eliable	Eliabte
0/56 long	Disable	100G Full	Down	Enable	Enable
Tolla					

```
(cs2) #
```

Restrictions and limitations - BES-53248 switches

Where problems arise when installing a license, the following debug commands should be run before running the copy command again to install the license.

Debug commands to use:

+ debug transfer debug license

```
(cs2) # debug transfer
Debug transfer output is enabled.
(cs2) # debug license
Enabled capability licensing debugging.
```

When you run the copy command with the debug transfer and debug license options enabled, the following log output is returned:

```
transfer.c(3083):Transfer process key or certificate file type = 43
transfer.c(3229):Transfer process key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
      "model": "BES-53248"
  },
  "description": "",
  "ports": "0+6"
  }
} .
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Model BES-53248 matched.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Applying license file 1.
```

Check for the following in the debug output:

- Check that the Serial number matches: Serial number QTFCU38290012 matched.
- Check that the switch Model matches: Model BES-53248 matched.
- Check that the specified license index was not used previously. Where a license index is already used, the following error is returned: License file /mnt/download//license.dat.1 already exists.
- A port license is not a feature license. Therefore, the following statement is expected: Feature not found in license file with index = 1.

Use the copy command to backup port licenses to the server:

```
(cs2) # copy nvram:license-key 1
scp://<UserName>@<IP_address>/saved_license_1.dat
```

See Installing licenses for BES-53248 cluster switches for details of the firmware versions supported for available licenses.



If you need to downgrade the switch software from version 3.4.4.6, the licenses are removed. This is expected behavior.

You must install an appropriate older license before reverting to an older version of the software.

Edit the Reference Configuration File (RCF) - BES-53248 switches

In order to activate newly licensed ports, you need to edit the latest version of the RCF and uncomment the applicable port details. The default license activates ports 0/1 to 0/16 and 0/55 to 0/56 while the newly licensed ports will be between ports 0/17 to 0/54 depending on the type and number of licenses available.

For details of the available license types for use on the BES-53248 cluster switch, see Installing licenses for BES-53248 cluster switches.

For example to activate the SW-BES54248-40-100G-LIC license, you must uncomment the following section in the RCF:

```
! 2-port or 6-port 40/100GbE node port license block
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
```

```
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
```

```
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
```



For high-speed ports between 0/49 to 0/54 inclusive, uncomment each port but only uncomment one **speed** line in the RCF for each of these ports, either:

- speed 100G full-duplex
- speed 40G full-duplex

as shown in the example.

For low-speed ports between 0/17 to 0/48 inclusive, uncomment the entire 8-port section when an appropriate license has been activated.

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the BES-53248 cluster switch for the first time and after the new license or licenses have been applied. If you are upgrading an RCF from an older version, you must reset the Broadcom switch settings and perform basic configuration to re-apply the RCF. You must perform this operation every time you want to upgrade or change an RCF. See the following KB article for details.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF.

If connectivity is an issue, use a nonrouted network and configure the service port using IP address

192.168.x or 172.19.x. You can reconfigure the service port to the production management IP address later

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Install the RCF on the BES-53248 cluster switch using the copy command.

```
(cs2) # copy http://172.19.2.1/tmp/BES-53248 RCF v1.6-Cluster-HA.txt
nvram:script BES-53248 RCF v1.6-Cluster-HA.scr
Remote Password ******
Mode..... HTTP
Path.....//tmp/
Filename..... BES-53248 RCF v1.6-
Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... BES-53248 RCF v1.6-
Cluster-HA.scr
File with same name already exists.
WARNING: Continuing with this command will overwrite the existing file.
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...
Validating configuration script...
[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```



Depending on your environment, you might need to use a double slash in the copy command, for example: copy http://172.19.2.1//tmp/BES-53248_RCF_v1.6-Cluster-HA.txt nvram:script BES-53248 RCF v1.6-Cluster-HA.scr.



The .scr extension must be set as part of the file name before invoking the script. This extension is the extension for the EFOS operating system. The switch validates the script automatically when it is downloaded to the switch, and the output goes to the console. Also, you can change the name of the .scr to fit your console screen for easier readability, for example: copy http://172.19.2.1/tmp/BES-53248_RCF_v1.6-Cluster-HA.txt nvram:script RCF v1.6-Cluster-HA.scr.

4. Verify that the script was downloaded and saved to the file name you gave it:

script list

5. Apply the script to the switch.

script apply

```
(cs2) # script apply BES-53248_RCF_v1.6-Cluster-HA.scr

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

The system has unsaved changes.

Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully .

Configuration Saved!

Configuration script 'BES-53248_RCF_v1.6-Cluster-HA.scr' applied.
```

6. Verify the ports for an additional license after the RCF is applied:

```
show port all | exclude Detach
```

```
(cs2) # show port all \| exclude Detach

Admin Physical Physical Link Link LACP

Actor
```

Intf Timeout	Type	Mode	Mode	Status	Status	Trap	Mode
0/1		Enable	Auto		Down	Enable	Enable
long 0/2		Enable	Auto		Down	Enable	Enable
long 0/3		Enable	Auto		Down	Enable	Enable
long 0/4		Enable	Auto		Down	Enable	Enable
long 0/5		Enable	Auto		Down	Enable	Enable
long							
0/6 long		Enable	Auto		Down	Enable	Enable
0/7 long		Enable	Auto		Down	Enable	Enable
0/8		Enable	Auto		Down	Enable	Enable
long 0/9		Enable	Auto		Down	Enable	Enable
long 0/10		Enable	Auto		Down	Enable	Enable
long 0/11		Enable	Auto		Down	Enable	Enable
long 0/12		Enable	Auto		Down	Enable	Enable
long 0/13		Enable	Auto		Down	Enable	Enable
long							
0/14 long		Enable	Auto		Down	Enable	Enable
0/15 long		Enable	Auto		Down	Enable	Enable
0/16 long		Enable	Auto		Down	Enable	Enable
0/49		Enable	40G Full		Down	Enable	Enable
long 0/50		Enable	40G Full		Down	Enable	Enable
long 0/51		Enable	100G Full		Down	Enable	Enable
long 0/52		Enable	100G Full		Down	Enable	Enable
long 0/53		Enable	100G Full		Down	Enable	Enable
long			_ 000 1011		2011		_114.0 1 0

0/54	Enable	100G Full	Down	Enable	Enable
long					
0/55	Enable	100G Full	Down	Enable	Enable
long					
0/56	Enable	100G Full	Down	Enable	Enable
long					

7. Verify on the switch that your changes have been made:

```
show running-config
```

```
(cs2) # show running-config
```

8. Save the running configuration so that it becomes the startup configuration when you reboot the switch:

```
write memory
```

```
(cs2) # 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!
```

9. Reboot the switch and verify that the running configuration is correct:

reload

```
(cs2) \# reload

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

System will now restart!
```

Configure the cluster switch log collection feature

The cluster switch health monitor log collection feature is used to collect switch-related log files in ONTAP. You must make sure that you have set up your environment using the BES-53248 cluster switch CLI as detailed here.

Steps

1. Generate the SSH keys:

crypto key generate

```
(switch) # show ip ssh
SSH Configuration
Administrative Mode: ..... Disabled
SSH Port: ...... 22
Protocol Level: ...... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA (521)
Key Generation In Progress: ..... None
SCP server Administrative Mode: ..... Disabled
(switch) # config
(switch) (Config) # crypto key generate rsa
Do you want to overwrite the existing RSA keys? (y/n): y
(switch) (Config) # crypto key generate dsa
Do you want to overwrite the existing DSA keys? (y/n): y
(switch) (Config) # crypto key generate ecdsa 521
Do you want to overwrite the existing ECDSA keys? (y/n): y
(switch) (Config) # aaa authorization commands "noCmdAuthList" none
(switch) (Config) # exit
(switch) # ip ssh server enable
(switch) # ip ssh pubkey-auth
(switch) # ip scp server enable
(switch) # write mem
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!
(switch) #
```

2. Verify that SSH is enabled:

show ip ssh

```
(switch) # show ip sshSSH ConfigurationEnabledAdministrative Mode:EnabledSSH Port:22Protocol Level:Version 2SSH Sessions Currently Active:0Max SSH Sessions Allowed:5SSH Timeout (mins):5Keys Present:DSA(1024) RSA(1024)ECDSA(521)Key Generation In Progress:NoneSCP server Administrative Mode:Disabled(switch) #
```

3. For ONTAP 9.8 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

system switch ethernet log setup-password system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```

4. For ONTAP 9.5P15, 9.6P11, 9.7P8 and later patch releases, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

system cluster-switch log setup-password system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

5. Begin an initial data collection from each switch:

```
° cluster1::*> system cluster-switch log collect -device <cs1>
° cluster1::*> system cluster-switch log collect -device <cs2>
```

Install the Cluster Switch Health Monitor (CSHM) configuration file

You can use this procedure to install the applicable configuration file for cluster switch health monitoring of BES-53248 cluster switches. In ONTAP releases 9.5P7 and earlier

and 9.6P2 and earlier, you must download the cluster switch health monitor configuration file separately. In ONTAP releases 9.5P8 and later, 9.6P3 and later, and 9.7 and later, the cluster switch health monitor configuration file is bundled with ONTAP.

What you'll need

Before you setup the switch health monitor for BES-53248 cluster switches, you must ensure that the ONTAP cluster is up and running.



It is advisable to enable SSH in order to use all features available in CSHM.

Steps

- 1. Download the cluster switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the page: NetApp Software download
 - a. On the Software download page, select Switch Health Monitor Configuration Files
 - b. Select Platform = **ONTAP** and click **Go!**
 - c. On the Switch Health Monitor Configuration Files for ONTAP page, click View & Download
 - d. On the Switch Health Monitor Configuration Files for ONTAP Description page, click **Download** for the applicable cluster switch model, for example: **Broadcom-supported BES-53248**
 - e. On the End User License Agreement page, click Accept
 - f. On the Switch Health Monitor Configuration Files for ONTAP Download page, select the applicable configuration file, for example, **Broadcom_BES-53248.zip**
- 2. Upload the applicable zip file to your internal web server where the IP address is X.X.X.X.

For an internal web server IP address of 192.168.2.20 and assuming a /usr/download directory exists, you can upload your zip file to your web server using scp:

```
% scp Broadcom_BES-53248.zip
admin@192.168.2.20:/usr/download/Broadcom_BES-53248.zip
```

3. Access the advanced mode setting from one of the ONTAP systems in the cluster, using the command set -privilege advanced:

```
cluster1::> set -privilege advanced
```

4. Run the switch health monitor configure command system cluster-switch configure-health-monitor -node * -package-url http://server/file-location:

```
cluster1::> system cluster-switch configure-health-monitor -node *
-package-url
http://192.168.2.20/usr/download/Broadcom_BES-53248.zip
```

5. Verify that the command output contains the text string "downloaded package processed successfully". If an error occurs, contact NetApp support.

6. Run the command system cluster-switch show on the ONTAP system and ensure that the cluster switches are discovered with the monitored field set to "True".

cluster1::> system cluster-switch show



If at any time you revert to an earlier version of ONTAP, you will need to install the CSHM configuration file again to enable switch health monitoring of BES-53248 cluster switches.

Migrate from CN1610 switches to BES-53248 switches

Migrate CN1610 cluster switches to Broadcom-supported BES-53248 cluster switches

You must be aware of certain configuration information, port connections, and cabling requirements when you migrate CN1610 cluster switches to Broadcom-supported BES-53248 cluster switches.

- The following cluster switches are supported:
 - · CN1610
 - · BES-53248
- The cluster switches support the following node connections:
 - NetApp CN1610: ports 0/1 through 0/12 (10 GbE)
 - BES-53248: ports 0/1-0/16 (10/25 GbE)



Additional ports can be activated by purchasing port licenses.

- The cluster switches use the following inter-switch link (ISL) ports:
 - NetApp CN1610: ports 0/13 through 0/16 (10 GbE)
 - BES-53248: ports 0/55-0/56 (100 GbE)
- The Hardware Universe contains information about ONTAP compatibility, supported EFOS firmware, and cabling to BES-53248 cluster switches.
- The appropriate ISL cabling is as follows:
 - Beginning: For CN1610 to CN1610 (SFP+ to SFP+), four SFP+ optical fiber or copper direct-attach cables.
 - Interim: For CN1610 to BES-53248 (SFP+ to SFP28), four 10G SFP+ optical transceiver/fiber or copper direct-attach cables.
 - **Final:** For BES-53248 to BES-53248 (QSFP28 to QSFP28), two QSFP28 optical transceivers/fiber or copper direct-attach cables.



After your migration completes, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for BES-53248 cluster switches.

See Installing the Cluster Switch Health Monitor (CSHM) configuration file in the Switch Setup and

Configuration Guide for Broadcom-supported BES-53248 switches guide.

See Configuring the cluster switch log collection feature in the Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches for the steps required to enable cluster health switch log collection used for collecting switch-related log files.

How to migrate CN1610 cluster switches to BES-53248 cluster switches - BES-53248 switches

To replace the existing CN1610 cluster switches in a cluster with Broadcom-supported BES-53248 cluster switches, you must perform a specific sequence of tasks.

What you'll need

The examples in this procedure use two nodes, each deploying two 10 GbE cluster interconnect ports: e0a and e0b.

The examples in this procedure use the following switch and node nomenclature:

- The command outputs might vary depending on different releases of ONTAP software.
- The CN1610 switches to be replaced are CL1 and CL2.
- The BES-53248 switches to replace the CN1610 switches are cs1 and cs2.
- The nodes are node1 and node2.
- The switch CL2 is replaced by cs2 first, followed with CL1 by cs1.
- The BES-53248 switches are pre-loaded with the supported versions of Reference Configuration File (RCF) and Ethernet Fabric OS (EFOS) with ISL cables connected on ports 55 and 56.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.

About this task

This procedure covers the following scenario:

- The cluster starts with two nodes connected to two CN1610 cluster switches.
- CN1610 switch CL2 is replaced by BES-53248 switch cs2:
 - Disconnect the cables from all cluster ports on all nodes connected to CL2, and then use supported cables to reconnect the ports to the new cluster switch cs2.
 - Disconnect the cables between ISL ports CL1 and CL2, and then use supported cables to reconnect the ports from CL1 to cs2.
- CN1610 switch CL1 is replaced by BES-53248 switch cs1:
 - Disconnect the cables from all cluster ports on all nodes connected to CL1, and then use supported cables to reconnect the ports to the new cluster switch cs1.
 - Disconnect the cables between ISL ports CL1 and cs2, and then use supported cables to reconnect the ports from cs1 to cs2.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

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

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster1::*> system node autosupport invoke -node \* -type all -message
MAINT=2h
```

2. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

3. Verify that auto-revert is enabled on all cluster LIFs:

network interface show -vserver Cluster -fields auto-revert

4. Display information about the devices in your configuration:

```
network device-discovery show -protocol cdp
```

The following example displays how many cluster interconnect interfaces have been configured in each node for each cluster interconnect switch:

		Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	CL2	0/2	CN1610
	e0b	CL1	0/2	CN1610
node1	/cdp			
	e0a	CL2	0/1	CN1610
	e0b	CL1	0/1	CN1610

- 5. Determine the administrative or operational status for each cluster interface.
 - a. Display the cluster network port attributes:

network port show -ipspace Cluster

cluster1:	:*> network p	ort show -:	ipspace	Clust	ter		
Node: nod	le1						
Ignore						Speed(Mbps)	Health
Health						opeca (Hops)	nearen
Status	IPspace					Admin/Oper	Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: nod	le2						
Ignore						Speed(Mbps)	Health
Status	IPspace						Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healthy
4 entries	were display	ed.					

b. Display information about the logical interfaces:

network interface show -vserver Cluster

```
cluster1::*> network interface show -vserver Cluster
         Logical Status Network
                                           Current
Current Is
Vserver Interface Admin/Oper Address/Mask
                                          Node
Port
     Home
______ _____
Cluster
         node1 clus1 up/up 169.254.209.69/16 node1
e0a
      true
         node1 clus2 up/up 169.254.49.125/16 node1
e0b
      true
         node2 clus1 up/up 169.254.47.194/16 node2
e0a
      true
         node2 clus2 up/up 169.254.19.183/16 node2
      true
e0b
4 entries were displayed.
```

- 6. Verify that the appropriate port licenses, RCF, and EFOS image are installed on the new BES-53248 switches as necessary for your requirements, and make any essential site customizations, such as users and passwords, network addresses, and so on.
- 7. Ping the remote cluster interfaces:

```
cluster ping-cluster -node node-name
```

The following example shows how to ping the remote cluster interfaces:

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
                                              e0a
Cluster node1 clus2 169.254.49.125 node1
                                              e0b
Cluster node2 clus1 169.254.47.194 node2
                                              e0a
Cluster node2 clus2 169.254.19.183 node2
                                             e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

8. Shut down the ISL ports 13 through 16 on the active CN1610 switch CL1:

shutdown

The following example shows how to shut down ISL ports 13 through 16 on the CN1610 switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface 0/13-0/16
(CL1) (Interface 0/13-0/16) # shutdown
(CL1) (Interface 0/13-0/16) # exit
(CL1) (Config) # exit
(CL1) #
```

9. Build a temporary ISL between CN1610 CL1 and new BES-53248 cs2. The ISL will only be defined on cs2 as the existing ISL on CL1 can be reused.

The following example builds a temporary ISL on cs2 (ports 13-16) to be connected to the existing ISL on CL1 (ports 13-16):

```
(cs2) # configure
(cs2) (Config) # port-channel name 1/2 temp-isl-cn1610
(cs2) (Config) # interface 0/13-0/16
(cs2) (Interface 0/13-0/16) # no spanning-tree edgeport
(cs2) (Interface 0/13-0/16) # addport 1/2
(cs2) (Interface 0/13-0/16) # exit
(cs2) (Config) # interface lag 2
(cs2) (Interface lag 2) # mtu 9216
(cs2) (Interface lag 2) # port-channel load-balance 7
(cs2) (Config) # exit
(cs2) # show port-channel 1/2
Channel Name..... temp-isl-cn1610
Link State..... Down
Admin Mode..... Enabled
Type..... Static
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr
      Device/
                 Port
                         Port
Ports
      Timeout
                 Speed
                        Active
______
0/13
    actor/long
                 10G Full False
      partner/long
0/14
    actor/long
                 10G Full False
      partner/long
0/15
      actor/long
                 10G Full False
      partner/long
0/16
      actor/long
                 10G Full False
      partner/long
```

10. On all nodes, remove the cables that are attached to the CN1610 switch CL2.

You must then reconnect the disconnected ports on all nodes to the new BES-53248 switch cs2. Refer to the *Hardware Universe* for approved cabling options.

11. Remove four ISL cables from ports 13 to 16 on the CN1610 switch CL2.

You must attach appropriate approved cabling connecting port 0/13 to 0/16 on the new BES-53248 switch cs2, to ports 13 to 16 on the existing CN1610 switch CL1.

12. Bring up ISLs 13 through 16 on the active CN1610 switch CL1.

The following example illustrates the process of bringing up ISL ports 13 through 16 on CL1:

```
(CL1) # configure

(CL1) (Config) # interface 0/13-0/16

(CL1) (Interface 0/13-0/16,3/1) # no shutdown

(CL1) (Interface 0/13-0/16,3/1) # exit

(CL1) (Config) # exit

(CL1) #
```

13. Verify that the ISLs are **up** on the CN1610 switch CL1:

show port-channel

The Link State should be Up, Type should be Static, and Port Active should be True for ports 0/13 to 0/16:

```
(CL2) # show port-channel 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr
     Device/
               Port
                      Port
               Speed
Ports
     Timeout
                      Active
0/13 actor/long 10 Gb Full True
    partner/long
0/14
    actor/long 10 Gb Full True
     partner/long
0/15
     actor/long 10 Gb Full True
     partner/long
0/16
     actor/long
              10 Gb Full True
     partner/long
```

14. Verify that the ISL ports are up on the BES-53248 switch:

show port-channel

```
(cs2) \# show port-channel 1/2
Channel Name..... temp-isl-cn1610
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Port-channel Min-links...... 1
Load Balance Option..... 7
(Src/Dest MAC, VLAN, EType, incoming port)
Mbr
     Device/
              Port
                     Port
Ports
     Timeout
              Speed
                     Active
0/13 actor/long
              10G Full True
     partner/long
    actor/long
0/14
              10G Full True
     partner/long
0/15
    actor/long
              10G Full True
     partner/long
     actor/long
0/16
              10G Full
                     True
     partner/long
```

15. Verify that all of the cluster interconnect ports are reverted to their home ports:

network interface show -vserver Cluster

			-vserver Cluster	Current	
G	Logical	Status	Network	Current	
Current Is	_			_	
Vserver	Interface	Admin/Oper	Address/Mask	Node	
Port Hom	ie				
	-				
Cluster					
	node1 clus1	up/up	169.254.209.69/16	node1	e0a
true	_	1. 1	,		
0140	node1 clus2	un/un	169.254.49.125/16	node1	e0b
true	nodei_crusz	αρ/ αρ	107.234.47.123/10	HOUCI	COD
crue	1 0 1 1	1	160 054 47 104/16	1 0	0
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					
4 entries w	ere displayed	_			

16. Verify that all of the cluster ports are connected:

network port show -ipspace Cluster

The following example shows the result of the previous command, verifying that all of the cluster interconnects are up:

cluster1:	:*> network p	ort show -	ipspace	Clus	ter		
Node: nod	e1						
Ignore						Speed(Mbps)	Uoolth
Health						speed (Mbps)	пеатип
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: nod	e2						
Ignore							
7.1						Speed(Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status	-					_	
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
false				-			_
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
	were display	ed.					

17. Ping the remote cluster interfaces:

cluster ping-cluster -node node-name

The following example shows how to ping the remote cluster interfaces:

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
Cluster node1 clus2 169.254.49.125 node1
                                               e0b
Cluster node2 clus1 169.254.47.194 node2
                                               e0a
Cluster node2 clus2 169.254.19.183 node2
                                               eob
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

18. On all nodes, remove the cables that are attached to the CN1610 switch CL1.

You must then reconnect the disconnected ports on all nodes to the new BES-53248 switch cs1. Refer to the *Hardware Universe* for approved cabling options.

- 19. Remove four ISL cables from ports 13 to 16 on BES-53248 switch cs2.
- 20. Remove the temporary port-channel 2 on cs2.

The following example removes port-channel 2 and copies the running-configuration file to the startup-configuration file:

```
(cs2) # configure
(cs2) (Config)# deleteport 1/2 all
(cs2) (Config)# interface 0/13-0/16
(cs2) (Interface 0/13-0/16)# spanning-tree edgeport
(cs2) (Interface 0/13-0/16)# exit
(cs2) (Config)# exit
(cs2) # 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 .
```

21. Verify the status of the cluster node port:

```
network port show -ipspace Cluster
```

The following example verifies that all of the cluster interconnect ports on node1 and node2 are up:

cluster1:	:*> network p	ort show -:	ipspace	Clus	ter		
Node: nod	e1						
Ignore						Speed(Mbps)	Health
Health						speed (Mpps)	nearch
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
Node: nod	e2						
Ignore						Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healthy
4 entries	were display	ed.					

22. Verify that the interface is now home:

network interface show -vserver Cluster

The following example shows the status of cluster interconnect interfaces are up and Is home for node1 and node2:

	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster		,	1.60 054 000 60/16		•
+	node1_clus1	up/up	169.254.209.69/16	nodel	e0a
true	node1 clus2	11n/11n	169.254.49.125/16	node1	e0b
true	110461_61432	ир/ ир	109.204.49.123/10	HOUCI	000
0100	node2 clus1	up/up	169.254.47.194/16	node2	e0a
true		-17-1			
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

23. Ping the remote cluster interfaces and then perform a remote procedure call server check:

cluster ping-cluster -node node-name

The following example shows how to ping the remote cluster interfaces:

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
Cluster node1 clus2 169.254.49.125 node1
                                               e0b
Cluster node2 clus1 169.254.47.194 node2
                                               e0a
Cluster node2 clus2 169.254.19.183 node2
                                               e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

24. Display the information about the devices in your configuration:

```
network device-discovery show -protocol cdp
```

The following examples show node1 and node2 have been migrated from CN1610 CL2 and CL1 to BES-53248 cs2 and cs1:

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node1	/cdp			
	e0a	cs2	0/1	BES-53248
	e0b	cs1	0/1	BES-53248
node2	/cdp			
	e0a	cs2	0/2	BES-53248
	e0b	cs1	0/2	BES-53248

25. Remove the replaced CN1610 switches if they are not automatically removed:

```
system cluster-switch delete -device device-name
```

The following example shows how to remove the CN1610 switches:

```
cluster::*> system cluster-switch delete -device CL2
cluster::*> system cluster-switch delete -device CL1
```

26. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

```
cluster::*> system node autosupport invoke -node \* -type all -message
MAINT=END
```

After you finish

See Configuring the cluster switch log collection feature in the Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches for the steps required to enable cluster health switch log collection used for collecting switch-related log files.

Related information

Hardware Universe

Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches

Migrate to a two-node switched cluster

Migrate to a two-node switched cluster with Broadcom-supported BES-53248 cluster switches

If you have a two-node switchless cluster, you can migrate, non-disruptively, to a two-node switched cluster that includes Broadcom-supported BES-53248 cluster switches. The documented process works for all cluster node ports using optical or Twinax ports but is not supported on this switch if nodes are using onboard 10GBASE-T RJ45 ports for the cluster network ports.

About this task

Most systems require two dedicated cluster-network ports on each controller.

Ensure that the BES-53248 cluster switch is set up as described in the Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches guide before starting this migration process.



After your migration completes, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for BES-53248 cluster switches.

See Installing the Cluster Switch Health Monitor (CSHM) configuration file in the Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches guide.

Also, see *Configuring the cluster switch log collection feature* in the Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches for the steps required to enable cluster health switch log collection used for collecting switch-related log files.

Migrate to a switched NetApp cluster environment using Broadcom-supported BES-53248 cluster switches

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using Broadcom-supported BES-53248 cluster switches to enable you to scale beyond two nodes in the cluster.

What you'll need

Two-node switchless configuration:

- The two-node switchless configuration must be properly set up and functioning.
- The nodes must be running ONTAP 9.5P8 and later. Support for 40/100 GbE cluster ports starts with EFOS firmware version 3.4.4.6 and later.
- All cluster ports must be in the up state.
- All cluster logical interfaces (LIFs) must be in the up state and on their home ports.

Broadcom-supported BES-53248 cluster switch configuration:

- The BES-53248 cluster switch must be fully functional on both switches.
- · Both switches must have management network connectivity.
- There must be console access to the cluster switches.
- BES-53248 node-to-node switch and switch-to-switch connections must use Twinax or fiber cables.

The NetAppHardware Universe contains information about ONTAP compatibility, supported EFOS

firmware, and cabling to BES-53248 switches.

Hardware Universe - Switches

- Inter-Switch Link (ISL) cables must be connected to ports 0/55 and 0/56 on both BES-53248 switches.
- Initial customization of both the BES-53248 switches must be completed. So that the:
 - BES-53248 switches are running the latest version of software
 - BES-53248 switches have optional port licenses installed, if purchased
 - Reference Configuration Files (RCFs) have been applied to the switches

Any site customization, such as SMTP, SNMP, and SSH must be configured on the new switches.

About this task

The examples in this procedure use the following cluster switch and node nomenclature:

- The names of the BES-53248 switches are cs1 and cs2.
- The names of the cluster SVMs are node1 and node2.
- The names of the LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- The cluster1::*> prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e0a and e0b.

The *Hardware Universe* contains the latest information about the actual cluster ports for your platforms.

Hardware Universe

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster1::*> system node autosupport invoke -node \* -type all -message
MAINT=2h
```

2. Change the privilege level to advanced, entering v when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

3. Disable all activated node-facing ports (not ISL ports) on both the new cluster switches cs1 and cs2.



You must not disable the ISL ports.

The following example shows that node-facing ports 1 through 16 are disabled on switch cs1:

```
(cs1) # configure
(cs1) (Config) # interface 0/1-0/16
(cs1) (Interface 0/1-0/16) # shutdown
(cs1) (Interface 0/1-0/16) # exit
(cs1) (Config) # exit
```

4. Verify that the ISL and the physical ports on the ISL between the two BES-53248 switches cs1 and cs2 are up:

```
show port-channel
```

The following example shows that the ISL ports are up on switch cs1:

```
(cs1) # show port-channel 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr Device/
            Port
                  Port
Ports Timeout
            Speed
                 Active
----- ------
0/55 actor/long
           100G Full True
   partner/long
0/56 actor/long
           100G Full True
    partner/long
(cs1) #
```

The following example shows that the ISL ports are up on switch cs2:

```
(cs2) # show port-channel 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links...... 1
(Enhanced hashing mode)
Mbr
   Device/
           Port
                 Port
Ports Timeout
          Speed
                Active
0/55 actor/long
          100G Full True
   partner/long
0/56 actor/long 100G Full True
   partner/long
(cs2) #
```

5. Display the list of neighboring devices:

```
show isdp neighbors
```

This command provides information about the devices that are connected to the system.

The following example lists the neighboring devices on switch cs1:

```
(cs1) # show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
                S - Switch, H - Host, I - IGMP, r - Repeater
             Intf Holdtime Capability Platform
                                                     Port ID
Device ID
                    176
cs2
             0/55
                              R
                                          BES-53248 0/55
cs2
             0/56
                     176
                             R
                                          BES-53248 0/56
```

The following example lists the neighboring devices on switch cs2:

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Intf Holdtime Capability Platform Port ID

cs2 0/55 176 R BES-53248 0/55

cs2 0/56 176 R BES-53248 0/56
```

6. Verify that all cluster ports are up:

network port show -ipspace Cluster

Each port should display up for Link and healthy for Health Status.

cluster1::*> network port show -ipspace Cluster Node: node1 Speed (Mbps) Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status up 9000 auto/10000 healthy e0a Cluster Cluster e0b Cluster Cluster up 9000 auto/10000 healthy Node: node2 Speed (Mbps) Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status up 9000 auto/10000 healthy e0a Cluster Cluster e0b Cluster Cluster up 9000 auto/10000 healthy 4 entries were displayed.

7. Verify that all cluster LIFs are up and operational: network interface show -vserver Cluster

Each cluster LIF should display true for Is Home and have a Status Admin/Oper of up/up

network in	terface sho	ow -vserver Cluster		
Logical	Status	Network	Current	
Interface	Admin/Oper	Address/Mask	Node	Port
_				
node1_clus1	up/up	169.254.209.69/16	node1	e0a
node1_clus2	up/up	169.254.49.125/16	node1	e0b
node2_clus1	up/up	169.254.47.194/16	node2	e0a
node2_clus2	up/up	169.254.19.183/16	node2	e0b
re displaye	ed.			
	Logical Interface node1_clus1 node1_clus2 node2_clus1	Logical Status Interface Admin/Oper node1_clus1 up/up node1_clus2 up/up node2_clus1 up/up	Logical Status Network Interface Admin/Oper Address/Mask	Interface Admin/Oper Address/Mask Node

8. Verify that auto-revert is enabled on all cluster LIFs: network interface show -vserver Cluster -fields auto-revert

9. Disconnect the cable from cluster port e0a on node1, and then connect e0a to port 1 on cluster switch cs1, using the appropriate cabling supported by the BES-53248 switches.

The NetApp Hardware Universe contains more information about cabling.

Hardware Universe - Switches

- 10. Disconnect the cable from cluster port e0a on node2, and then connect e0a to port 2 on cluster switch cs1, using the appropriate cabling supported by the BES-53248 switches.
- 11. Enable all node-facing ports on cluster switch cs1.

The following example shows that ports 1 through 16 are enabled on switch cs1:

```
(cs1) # configure
(cs1) (Config) # interface 0/1-0/16
(cs1) (Interface 0/1-0/16) # no shutdown
(cs1) (Interface 0/1-0/16) # exit
(cs1) (Config) # exit
```

12. Verify that all cluster LIFs are up, operational, and display as true for Is Home:

```
network interface show -vserver Cluster
```

The following example shows that all of the LIFs are up on node1 and node2 and that Is Home results are true:

cluster1	::*> network	interface sl	how -vserver Cluste	r	
	Logical	Status	Network	Current	Current
Is					
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster		,	1.00 0.5 1.000 0.0 /1.0		
.	node1_clus1	up/up	169.254.209.69/16	nodel	e0a
true true	node1_clus2	up/up	169.254.49.125/16	node1	e0b
crue	node2 clus1	מנו/מנו	169.254.47.194/16	node2	e0a
true	110402_01401	αρ/ αρ	103.201.17.131,10	110002	00 u
	node2 clus2	up/up	169.254.19.183/16	node2	e0b
true	<u> </u>				
4 entrie	s were displa	yed.			

13. Display information about the status of the nodes in the cluster:

```
cluster show
```

The following example displays information about the health and eligibility of the nodes in the cluster:

- 14. Disconnect the cable from cluster port e0b on node1, and then connect e0b to port 1 on cluster switch cs2, using the appropriate cabling supported by the BES-53248 switches.
- 15. Disconnect the cable from cluster port e0b on node2, and then connect e0b to port 2 on cluster switch cs2, using the appropriate cabling supported by the BES-53248 switches.
- 16. Enable all node-facing ports on cluster switch cs2.

The following example shows that ports 1 through 16 are enabled on switch cs2:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)# exit
```

17. Verify that all cluster ports are up:

```
network port show -ipspace Cluster
```

The following example shows that all of the cluster ports are up on node1 and node2:

cluster1:	:*> network p	ort show -i	.pspace	Clust	ter		
Node: node	e1						
Ignore						a 1/24	
Health						Speed (Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
Node: node	e2						
Ignore							
						Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
 e0a	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
4 entries	were displaye	ed.					

18. Verify that all interfaces display true for Is Home:

network interface show -vserver Cluster



This might take several minutes to complete.

The following example shows that all LIFs are up on node1 and node2 and that Is Home results are true:

cluster1:	:*> network i	nterface sh	ow -vserver Cluster		
	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					
4 entries	were display	ed.			

19. Verify that both nodes each have one connection to each switch:

show isdp neighbors

The following example shows the appropriate results for both switches:

(cs1)# show isdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater Intf Holdtime Capability Platform -- Port ID Device ID 0/1 node1 175 Н FAS2750 e0a FAS2750 e0a 0/2 Н node2 157 cs2 0/55 178 R BES-53248 0/55 cs2 0/56 178 R BES-53248 0/56 (cs2) # show isdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater Device ID Intf Holdtime Capability Platform Port ID node1 0/1 137 Н FAS2750 e0b node2 0/2 Н 179 FAS2750 e0b R cs1 0/55 175 BES-53248 0/55 cs1 0/56 175 R BES-53248 0/56

20. Display information about the discovered network devices in your cluster:

network device-discovery show -protocol cdp

		Discovered Device (LLDP: ChassisID)	Interface	Platform
				1100101111
node2	/cdp			
	e0a	cs1	0/2	BES-53248
	e0b	cs2	0/2	BES-53248
node1	/cdp			
	e0a	cs1	0/1	BES-53248
	e0b	cs2	0/1	BES-53248
			·	

21. Verify that the settings are disabled:



It might take several minutes for the command to complete. Wait for the '3 minute lifetime to expire' announcement.

The false output in the following example shows that the configuration settings are disabled:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

22. Verify the status of the node members in the cluster:

cluster show

The following example shows information about the health and eligibility of the nodes in the cluster:

cluster1::*> cluster	show		
Node	Health	Eligibility	Epsilon
node1 node2	true true	true true	false

23. Ensure that the cluster network has full connectivity using the command:

cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 192.168.168.26 node1 e0a
Cluster node1 clus2 192.168.168.27 node1 e0b
Cluster node2 clus1 192.168.168.28 node2 e0a
Cluster node2 clus2 192.168.168.29 node2 e0b
Local = 192.168.168.28 192.168.168.29
Remote = 192.168.168.26 192.168.168.27
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 4 path(s):
    Local 192.168.168.28 to Remote 192.168.168.26
    Local 192.168.168.28 to Remote 192.168.168.27
    Local 192.168.168.29 to Remote 192.168.168.26
    Local 192.168.168.29 to Remote 192.168.168.27
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

24. Change the privilege level back to admin:

```
set -privilege admin
```

25. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

```
cluster1::*> system node autosupport invoke -node \* -type all -message
MAINT=END
```

After you finish

See Configuring the cluster switch log collection feature in the Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches for the steps required to enable cluster health switch log collection used for collecting switch-related log files.

Related information

Hardware Universe

NetApp KB Article: How to suppress automatic case creation during scheduled maintenance windows

Upgrade a switch in an NDO/NDU environment

Upgrade a BES-53248 cluster switch in an NDO/NDU environment

Upgrading BES-53248 cluster switches starts with preparing the controller for upgrade, installing the EFOS software, licenses, and reference configuration file (RCF). After the installation, you can restore the controller configuration in a nondisruptive upgrade (NDU) and nondisruptive operation (NDO) environment.

What you'll need

The following conditions must exist before you install the EFOS software, licenses, and the RCF file on an existing NetApp BES-53248 cluster switch:

- The cluster must be a fully functioning cluster (no error log messages or other issues).
- The cluster must not contain any defective cluster network interface cards (NICs).
- All connected ports on both cluster switches must be functional.
- · All cluster ports must be up.
- All cluster LIFs must be administratively and operationally up and on their home ports.
- The ONTAP cluster ping-cluster -node node1 advanced privilege command must indicate that larger than PMTU communication is successful on all paths.
- There might be command dependencies between command syntax in the RCF and EFOS versions.

About this task

You must consult the switch compatibility table on the NetApp BES-53248 switches page for the supported EFOS, RCF, and ONTAP versions at: NetApp BES-53248 switches.

This procedure applies to a functioning cluster and allows for NDU and NDO. The examples in this procedure use the following switch and node nomenclature:

- The NetApp switch names are cs1 and cs2.
- The example used in this procedure starts the upgrade on the second switch, cs2.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The IPspace name is Cluster.
- The cluster1::> prompt indicates the name of the cluster.
- The cluster ports on each node are named e0a and e0b.

See the *Hardware Universe* for the actual cluster ports supported on your platform.

NetApp Hardware Universe

• The Inter-Switch Links (ISLs) supported for the NetApp cluster switches are ports 0/55 and 0/56.

- The node connections supported for the NetApp cluster switches are ports 0/1 through 0/16 with default licensing.
- The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.
- Repeat all procedures in this section to upgrade the EFOS software and RCF file on the other switch, cs1.

Prepare the controller for a cluster switch upgrade

You can use this procedure to prepare the controller for a BES-53248 cluster switch upgrade.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF.

If this is an issue, use a nonrouted network and configure the service port using IP address 192.168.x or 172.19.x. You can reconfigure the service port to the production management IP address later.

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Verify that the cluster ports are healthy and have a link using the command:

```
network port show -ipspace Cluster
```

The following example shows the type of output with all ports having a Link value of up and a Health Status of healthy:

<pre>cluster1::> network port show -ipspace Cluster</pre>									
Node:	Node: node1								
Ignore						Crood (Mbra)	IIo al + b		
Health						Speed (Mbps)	пеатсп		
	IPspace					_			
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy		
	Cluster	Cluster		up	9000	auto/10000	healthy		
false									
Node:									
_						Speed(Mbps)	Health		
Health Port Status	IPspace					Admin/Oper			
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy		
	Cluster	Cluster		up	9000	auto/10000	healthy		
4 entries were displayed.									

4. Verify that the cluster LIFs are administratively and operationally up and reside on their home ports, using the command:

network interface show -vserver Cluster

In this example, the -vserver parameter displays information about the LIFs that are associated with cluster ports. Status Admin/Oper must be up and Is Home must be true:

<pre>cluster1::> network interface show -vserver Cluster</pre>							
	Logical	Status	Network	Current			
Current I	S						
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port		
Home							
Cluster							
	node1_clus1						
		up/up	169.254.217.125/16	node1	e0a		
true							
	node1_clus2						
		up/up	169.254.205.88/16	node1	e0b		
true							
	node2_clus1						
		up/up	169.254.252.125/16	node2	e0a		
true							
	node2_clus2						
		up/up	169.254.110.131/16	node2	e0b		
true							
4 entries were displayed.							

Install the EFOS software

You can use this procedure to install the EFOS software on the BES-53248 cluster switch. You can download the applicable Broadcom EFOS software for your cluster switches from the Broadcom Ethernet Switch Support site.

About this task

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
	FIPS compliant	Non-FIPS compliant	and license information will be lost.



Note that after upgrading BES-53248 cluster switches from EFOS 3.3.x.x or 3.4.x.x to EFOS 3.7.0.4 or 3.8.0.2, Inter-Switch Links (ISLs) and port channels are marked in the **Down** state. See this KB article for further details.

Steps

- 1. Connect the BES-53248 cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF file.

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Back up the current active image on cs2:

show bootvar

(cs2) # show bootvar Image Descriptions active : backup : Images currently available on Flash ______ unit active backup current-active next-active 1 3.4.3.3 Q.10.22.1 3.4.3.3 3.4.3.3 (cs2) # copy active backup Copying active to backup Management access will be blocked for the duration of the operation Copy operation successful (cs2) # show bootvar Image Descriptions active : backup : Images currently available on Flash _____ active backup current-active next-active 1 3.4.3.3 3.4.3.3 3.4.3.3 3.4.3.3 (cs2) #

4. Verify the running version of the EFOS software:

show version

(cs2) # show version
Switch: 1
System Description Quanta IX8-B 48x25GB SFP
8x100GB QSFP, 3.4.3.3, Linux 4.4.117-ceeeb99d, 2016.05.00.04
Machine Type Quanta IX8-B 48x25GB SFP
8x100GB QSFP
Machine Model IX8-B
Serial Number QTFCU38260014
Maintenance Level A
Manufacturer 0xbc00
Burned In MAC Address D8:C4:97:71:12:3D
Software Version 3.4.3.3
Operating System Linux 4.4.117-ceeeb99d
Network Processing Device BCM56873_A0
CPLD Version 0xff040c03
Additional Packages BGP-4
QOS
Multicast
IPv6
Routing
Data Center
Open Api
Prototype Open API

5. Download the image file to the switch.

Copying the image file to the active image means that when you reboot, that image establishes the running EFOS version. The previous image remains available as a backup.

6. Display the boot images for the active and backup configuration:

show bootvar

(cs2) # show bootvar Image Descriptions active : backup : Images currently available on Flash ______ unit active backup current-active next-active _____ 1 3.4.3.3 3.4.3.3 3.4.3.3 3.4.4.6

7. Reboot the switch:

reload

```
(cs2) # reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully .
Configuration Saved!
System will now restart!
```

8. Log in again and verify the new version of the EFOS software:

show version

```
(cs2) # show version
Switch: 1
System Description..... x86 64-
quanta common rglbmc-r0, 3.4.4.6, Linux 4.4.211-28a6fe76, 2016.05.00.04
Machine Type..... x86 64-
quanta common rglbmc-r0
Machine Model..... BES-53248
Maintenance Level..... A
Burned In MAC Address..... D8:C4:97:71:0F:40
Operating System..... Linux 4.4.211-28a6fe76
Network Processing Device..... BCM56873 A0
Additional Packages..... BGP-4
..... QOS
..... Multicast
..... IPv6
..... Routing
..... Data Center
 ..... Open Api
 ..... Prototype Open API
```

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.



This functionality is only available for EFOS 3.7.x.x or later non-FIPS compliant.

Steps

1. Boot the switch into ONIE installation mode.

During boot, select ONIE when the following screen appears:

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

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:

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

7. Complete the installation.

The switch will reboot with no configuration applied and reset to factory defaults.

Related information

Broadcom Ethernet Switch Support

Install licenses for BES-53248 cluster switches

The BES-53248 cluster switch base model is licensed for 16 10GbE or 25GbE ports and two 100GbE ports. New ports can be added by purchasing more licenses.

The following licenses are available for use on the BES-53248 cluster switch:

License type	License details
Supported firmware version	SW-BES-53248A1-G1-8P-LIC
Broadcom 8P 10-25,2P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES-53248A1-G1-16P-LIC	Broadcom 16P 10-25,4P40-100 License Key, X190005/R
EFOS 3.4.3.3 and later	SW-BES-53248A1-G1-24P-LIC
Broadcom 24P 10-25,6P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES54248-40-100G-LIC	Broadcom 6Port 40G100G License Key, X190005/R
EFOS 3.4.4.6 and later	SW-BES53248-8P-10G25G-LIC
Broadcom 8Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later
SW-BES53248-16P-1025G-LIC	Broadcom 16Port 10G25G License Key, X190005/R
EFOS 3.4.4.6 and later	SW-BES53248-24P-1025G-LIC
Broadcom 24Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF file.

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Check the current license usage on switch cs2:

show license

4. Install the license file. The following example uses SFTP to copy a license file to a key index 1.

Repeat this step to load more licenses and to use different key index numbers.

5. Display all current license information and note the license status before switch cs2 is rebooted:

show license

6. Display all licensed ports:

```
show port all | exclude Detach
```

The ports from the additional license files are not displayed until after the switch is rebooted.

(cs2) # s	(cs2) # show port all \ exclude Detach							
		Admin	Physical	Physical	Link	Link	LACP	
Actor Intf	Type	Mode	Mode	Status	Status	Trap	Mode	
Timeout								
0/1		Disable	Auto		Down	Enable	Enable	
long 0/2		Disable	Auto		Down	Enable	Enable	
long		DISADIC	Auco		DOWII	Enable	HIRDIC	
0/3		Disable	Auto		Down	Enable	Enable	
long					_			
0/4 long		Disable	Auto		Down	Enable	Enable	
0/5		Disable	Auto		Down	Enable	Enable	
long								
0/6		Disable	Auto		Down	Enable	Enable	
long					_	_ ,,	_ ,,	
0/7 long		Disable	Auto		Down	Enable	Enable	
0/8		Disable	Auto		Down	Enable	Enable	
long								
0/9		Disable	Auto		Down	Enable	Enable	
long		Disable	7.1.+0		Dorra	Enchlo	Enable	
0/10 long		DISADIE	Auto		Down	Enable	Ellable	
0/11		Disable	Auto		Down	Enable	Enable	
long								
0/12		Disable	Auto		Down	Enable	Enable	
long 0/13		Disable	Auto		Down	Enable	Enable	
long								
0/14		Disable	Auto		Down	Enable	Enable	
long		D-1 1 - 1 -	7		Dan	Emple 1	En ala l	
0/15 long		Disable	Auto		Down	Enable	Enable	
0/16		Disable	Auto		Down	Enable	Enable	
long								
0/55		Disable	Auto		Down	Enable	Enable	
long		Diasi-1-	7		Dan	Emple 1	Enable	
0/56 long		Disable	Auto		Down	Enable	Enable	
9								

7. Reboot the switch:

reload

```
(cs2) # reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully .
Configuration Saved!
Are you sure you would like to reset the system? (y/n) y
```

8. Check that the new license is active and note that the license has been applied:

show license

9. Check that all new ports are available:

show port all | exclude Detach

```
(cs2) # show port all \| exclude Detach

Admin Physical Physical Link Link LACP

Actor
Intf Type Mode Mode Status Status Trap Mode

Timeout
------
0/1 Disable Auto Down Enable Enable
long
```

0/2 long	Disable	Auto	Down	Enable	Enable
0/3	Disable	Auto	Down	Enable	Enable
long 0/4	Disable	Auto	Down	Enable	Enable
long 0/5	Disable	Auto	Down	Enable	Enable
long 0/6	Disable	Auto	Down	Enable	Enable
long 0/7	Disable	Auto	Down	Enable	Enable
long 0/8	Disable	Auto	Down	Enable	Enable
long 0/9	Disable	Auto	Down	Enable	Enable
long 0/10	Disable	Auto	Down	Enable	Enable
long 0/11	Disable	Auto	Down	Enable	Enable
long 0/12	Disable	Auto	Down	Enable	Enable
long 0/13	Disable	Auto	Down	Enable	Enable
long 0/14	Disable	Auto	Down	Enable	Enable
long 0/15	Disable	Auto	Down	Enable	Enable
long 0/16	Disable	Auto	Down	Enable	Enable
long 0/49	Disable	100G Full	Down	Enable	Enable
long 0/50	Disable	100G Full	Down	Enable	Enable
long 0/51	Disable	100G Full	Down	Enable	Enable
long 0/52	Disable	100G Full	Down	Enable	Enable
long 0/53	Disable	100G Full	Down	Enable	Enable
long 0/54	Disable	100G Full	Down	Enable	Enable
long 0/55	Disable	100G Full	Down	Enable	Enable
long 0/56	Disable	100G Full	Down	Enable	Enable
long					

```
(cs2) #
```

Restrictions and limitations - BES-53248 switches

Where problems arise when installing a license, the following debug commands should be run before running the <code>copy</code> command again to install the license.

Debug commands to use:

debug transferdebug license

```
(cs2) # debug transfer
Debug transfer output is enabled.
(cs2) # debug license
Enabled capability licensing debugging.
```

When you run the copy command with the debug transfer and debug license options enabled, the following log output is returned:

```
transfer.c(3083):Transfer process key or certificate file type = 43
transfer.c(3229):Transfer process key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
     "model": "BES-53248"
  },
  "description": "",
  "ports": "0+6"
  }
} .
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Model BES-53248 matched.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING: Fri Sep 11 13:41:32 2020: Applying license file 1.
```

Check for the following in the debug output:

- Check that the Serial number matches: Serial number QTFCU38290012 matched.
- Check that the switch Model matches: Model BES-53248 matched.
- Check that the specified license index was not used previously. Where a license index is already used, the following error is returned: License file /mnt/download//license.dat.1 already exists.
- A port license is not a feature license. Therefore, the following statement is expected: Feature not found in license file with index = 1.

Use the copy command to backup port licenses to the server:

```
(cs2) # copy nvram:license-key 1
scp://<UserName>@<IP_address>/saved_license_1.dat
```

See Installing licenses for BES-53248 cluster switches for details of the firmware versions supported for available licenses.



If you need to downgrade the switch software from version 3.4.4.6, the licenses are removed. This is expected behavior.

You must install an appropriate older license before reverting to an older version of the software.

Edit the Reference Configuration File (RCF)

In order to activate newly licensed ports, you need to edit the latest version of the RCF and uncomment the applicable port details. The default license activates ports 0/1 to 0/16 and 0/55 to 0/56 while the newly licensed ports will be between ports 0/17 to 0/54 depending on the type and number of licenses available.



If you try to edit a previously installed RCF, the process might fail because there is an existing configuration for other areas in the RCF, see Edit a previously installed RCF file.

For details of the available license types for use on the BES-53248 cluster switch, see Installing licenses for BES-53248 cluster switches.

For example to activate the SW-BES54248-40-100G-LIC license, you must uncomment the following section in the RCF:

```
! 2-port or 6-port 40/100GbE node port license block
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED 100G
```

```
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
```

```
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED 100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
```



For high-speed ports between 0/49 to 0/54 inclusive, uncomment each port but only uncomment one **speed** line in the RCF for each of these ports, either:

- speed 100G full-duplex
- speed 40G full-duplex

as shown in the example.

For low-speed ports between 0/17 to 0/48 inclusive, uncomment the entire 8-port section when an appropriate license has been activated.

Edit a previously installed RCF file

After you edit a previously installed RCF file and run the script apply command, you might get the following error message:

```
(CS1) \#script apply BES-53248_RCF_v1.6-Cluster-HA.scr Are you sure you want to apply the configuration script? (y/n)
```

After you select y, you get the following error message:

```
config
...
match cos 5
Unrecognized command: match cos 5
Error! in configuration script file at line number 40.
CLI Command:: match cos 5.
Aborting script.
```

To either avoid or resolve this issue, you can choose one of the following options:

- To avoid the error, you can use following procedure:
 - 1. Create a second a RCF file containing the new port configuration only.
 - 2. Copy the second RCF file to the switch.
 - 3. Apply the script to the switch:

```
script apply
```

 To resolve the error, see the Knowledge Base article: Error! in configuration script file at line number XX when applying a new RCF

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the BES-53248 cluster switch for the first time and after the new license or licenses have been applied. If you are upgrading an RCF from an older version, you must reset the Broadcom switch settings and perform basic configuration to re-apply the RCF. You must perform this operation every time you want to upgrade or change an RCF. See the following KB article for details.

Reset 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 cluster switches.
- 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

```
(cs2)> enable (cs2) #
```

2. Erase the startup configuration and remove the banner

a. Erase the startup configuration:

erase startup-config

```
(cs2) #erase startup-config
Are you sure you want to clear the configuration? (y/n) y
(cs2) #
```

This command does not erase the banner.

b. Remove the banner:

no set clibanner

```
(cs2) #configure
(cs2)(Config) # no set clibanner
(cs2)(Config) #
```

3. Reboot the switch:

(cs2) #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:

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 cs2

The switch prompt will display the new name:

```
(Routing) # hostname cs2
(cs2) #
```

13. Save the configuration:

write memory

You receive prompts and output similar to the following example:

```
(cs2) #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!
(cs2) #
```

14. Repeat the previous steps on the other cluster switch.

Install the Reference Configuration File (RCF)

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting EFOS, licenses, and the RCF.

If connectivity is an issue, use a nonrouted network and configure the service port using IP address 192.168.x or 172.19.x. You can reconfigure the service port to the production management IP address later.

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2) # ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Install the RCF on the BES-53248 cluster switch using the copy command.

```
(cs2) # copy http://172.19.2.1/tmp/BES-53248 RCF v1.6-Cluster-HA.txt
nvram:script BES-53248 RCF v1.6-Cluster-HA.scr
Remote Password ******
Mode..... HTTP
Path.....//tmp/
Filename..... BES-53248 RCF v1.6-
Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... BES-53248 RCF v1.6-
Cluster-HA.scr
File with same name already exists.
WARNING: Continuing with this command will overwrite the existing file.
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...
Validating configuration script...
[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```



Depending on your environment, you might need to use a double slash in the copy command, for example: copy http://172.19.2.1//tmp/BES-53248_RCF_v1.6-Cluster-HA.txt nvram:script BES-53248 RCF v1.6-Cluster-HA.scr.



The .scr extension must be set as part of the file name before invoking the script. This extension is the extension for the EFOS operating system. The switch validates the script automatically when it is downloaded to the switch, and the output goes to the console. Also, you can change the name of the .scr to fit your console screen for easier readability, for example: copy http://172.19.2.1/tmp/BES-53248_RCF_v1.6-Cluster-HA.txt nvram:script RCF v1.6-Cluster-HA.scr.

4. Verify that the script was downloaded and saved to the file name you gave it:

script list

5. Apply the script to the switch.

```
script apply
```

```
(cs2) # script apply BES-53248_RCF_v1.6-Cluster-HA.scr

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

The system has unsaved changes.

Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully .

Configuration Saved!

Configuration script 'BES-53248_RCF_v1.6-Cluster-HA.scr' applied.
```

6. Verify the ports for an additional license after the RCF is applied:

```
show port all | exclude Detach
```

```
(cs2) # show port all \| exclude Detach

Admin Physical Physical Link Link LACP

Actor
```

O/1	Intf Timeout	Type	Mode	Mode	Status	Status	Trap	Mode
10ng								
0/2 Enable Auto Down Enable Enable 10ng 0/3 Enable Auto Down Enable Enable 10ng 0/4 Enable Auto Down Enable Enable 10ng 0/5 Enable Auto Down Enable Enable 10ng 0/6 Enable Auto Down Enable Enable 10ng 0/7 Enable Auto Down Enable Enable 10ng 0/8 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/10 Enable Auto Down Enable Enable 10ng 0/11 Enable Auto	0/1		Enable	Auto		Down	Enable	Enable
10ng	-							
O/3			Enable	Auto		Down	Enable	Enable
10ng 0/4 Enable Auto Down Enable Enable 10ng 0/5 Enable Auto Down Enable Enable 10ng 0/6 Enable Auto Down Enable Enable 10ng 0/7 Enable Auto Down Enable Enable 10ng 0/7 Enable Auto Down Enable Enable 10ng 0/8 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/10 Enable Auto Down Enable Enable 10ng 0/11 Enable Auto Down Enable Enable 10ng 0/12 Enable Auto Down Enable Enable 10ng 0/13 Enable Auto Down Enable Enable 10ng 0/14 Enable Auto Down Enable Enable 10ng 0/15 Enable Auto Down Enable Enable 10ng 0/16 Enable Auto Down Enable Enable 10ng 0/50 Enable 40G Full Down Enable Enable 10ng 0/51 Enable 100G Full Down Enable Enable 10ng 0/52 Enable 100G Full Down Enable Enable 10ng 0/52 Enable 100G Full Down Enable Enable 10ng 0/53 Enable 100G Full Down Enable Enable Enable	-		En ala la	7		D	Trable	The shale
0/4 Enable Auto Down Enable Enable long 0/5 Enable Auto Down Enable Enable long 0/6 Enable Auto Down Enable Enable long 0/7 Enable Auto Down Enable Enable long 0/8 Enable Auto Down Enable Enable long 0/9 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/17 Enable Auto Down Enable Enable long 0/18 Enable Auto Down Enable Enable long 0/19 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/19 Enable 40G Full Down Enable Enable long 0/50 Enable 100G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable Enable			Ellabie	Auto		DOWII	Eliable	Ellabite
0/5 Enable Auto Down Enable Enable long 0/6 Enable Auto Down Enable Enable Enable long 0/7 Enable Auto Down Enable Enable long 0/7 Enable Auto Down Enable Enable long 0/8 Enable Auto Down Enable Enable long 0/9 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable Enable	_		Enable	Auto		Down	Enable	Enable
long 0/6	long							
0/6 Enable Auto Down Enable Enable long 0/7 Enable Auto Down Enable Enable long 0/8 Enable Auto Down Enable Enable long 0/9 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/17 Enable Auto Down Enable Enable long 0/18 Enable Auto Down Enable Enable long 0/19 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable Enable long 0/10 Enable Enable Enable Enable Enable Enable Enable long			Enable	Auto		Down	Enable	Enable
long 0/7 Enable Auto Down Enable Enable long 0/8 Enable Auto Down Enable Enable Enable long 0/9 Enable Auto Down Enable Enable long 0/9 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Enable long 0/16 Enable Enable Enable long 0/16 Enable Enable Enable long 0/16 Enable Enable Enable Enable long 0/16 Enable Enable Enable Enable Enable Enable Enable Long 0/16 Enable Enable Enable Enable Enable Enable Long 0/16 Enable Enable Enable Enable Enable Enable Long 0/16 Enable Enable Enable Enable Enable Enable Enable Enable Enable Long 0/16 Enable Ena	_		- 11			-	- 11	- 13
0/7 Enable Auto Down Enable Enable long 0/8 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/10 Enable Auto Down Enable Enable 10ng 0/11 Enable Auto Down Enable Enable 10ng 0/12 Enable Auto Down Enable Enable 10ng 0/13 Enable Auto Down Enable Enable 10ng 0/14 Enable Auto Down Enable Enable 10ng 0/15 Enable Auto Down Enable Enable 10ng 0/16 Enable Auto Down Enable Enable 10ng 0/17 Enable Auto Down Enable Enable 10ng 0/18 Enable Auto Down Enable Enable 10ng 0/19 Enable Auto Down Enable Enable 10ng 0/50 Enable Aug Full Down Enable Enable 10ng 0/51 Enable 100G Full Down Enable Enable 10ng 0/52 Enable 100G Full Down Enable Enable			Enable	Auto		Down	Enable	Enable
10ng 0/8 Enable Auto Down Enable Enable 10ng 0/9 Enable Auto Down Enable Enable 10ng 0/10 Enable Auto Down Enable Enable 10ng 0/10 Enable Auto Down Enable Enable 10ng 0/11 Enable Auto Down Enable Enable 10ng 0/12 Enable Auto Down Enable Enable 10ng 0/13 Enable Auto Down Enable Enable 10ng 0/14 Enable Auto Down Enable Enable 10ng 0/15 Enable Auto Down Enable Enable 10ng 0/16 Enable 40G Full Down Enable Enable 10ng 0/50 Enable 40G Full Down Enable Enable 10ng 0/51 Enable 100G Full Down Enable Enable 10ng 0/52 Enable 100G Full Down Enable Enable 10ng 0/52 Enable 100G Full Down Enable Enable 10ng 0/53 Enable 100G Full Down Enable Enable Enable	-		Enable	Auto		Down	Enable	Enable
long 0/9 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/17 Enable Auto Down Enable Enable long 0/18 Enable Auto Down Enable Enable Enable long 0/18 Enable Enable Ing 0/18 Enable Ing								
0/9 Enable Auto Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/19 Enable Auto Down Enable Enable long 0/10 Down Enable Enable long 0/10 Enable Auto Down Enable Enable long 0/11 Down Enable Enable long 0/12 Enable Enable Ing 0/13 Enable Ing Full Down Enable Enable long 0/50 Enable Ing Full Down Enable Enable long 0/51 Enable Ing Full Down Enable Enable long 0/52 Enable Ing Full Down Enable Enable long 0/53 Enable Ing Full Down Enable Enable	0/8		Enable	Auto		Down	Enable	Enable
1 long 0/10	-					_		
0/10 Enable Auto Down Enable Enable long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable			Enable	Auto		Down	Enable	Enable
long 0/11 Enable Auto Down Enable Enable long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	-		Enable	Auto		Down	Enable	Enable
long 0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable								
0/12 Enable Auto Down Enable Enable long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	0/11		Enable	Auto		Down	Enable	Enable
long 0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	_							
0/13 Enable Auto Down Enable Enable long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable			Enable	Auto		Down	Enable	Enable
long 0/14 Enable Auto Down Enable Enable long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	_		Enable	Auto		Down	Enable	Enable
long 0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable						-		
0/15 Enable Auto Down Enable Enable long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	0/14		Enable	Auto		Down	Enable	Enable
long 0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	_							
0/16 Enable Auto Down Enable Enable long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable			Enable	Auto		Down	Enable	Enable
long 0/49 Enable 40G Full Down Enable Enable long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	_		Enable	Auto		Down	Enable	Enable
long 0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable								
0/50 Enable 40G Full Down Enable Enable long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	0/49		Enable	40G Full		Down	Enable	Enable
long 0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	-							
0/51 Enable 100G Full Down Enable Enable long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable			Enable	40G Full		Down	Enable	Enable
long 0/52 Enable 100G Full Down Enable Enable long 0/53 Enable 100G Full Down Enable Enable	_		Enable	100G Full		Down	Enable	Enable
long 0/53 Enable 100G Full Down Enable Enable								
0/53 Enable 100G Full Down Enable Enable	_		Enable	100G Full		Down	Enable	Enable
	-							
TOIIG			Enable	100G Full		Down	Enable	Enable
	Toud							

0/54	Enable	100G Full	Down	Enable	Enable
long					
0/55	Enable	100G Full	Down	Enable	Enable
long					
0/56	Enable	100G Full	Down	Enable	Enable
long					

7. Verify on the switch that your changes have been made:

```
show running-config
```

```
(cs2) # show running-config
```

8. Save the running configuration so that it becomes the startup configuration when you reboot the switch:

```
write memory
```

```
(cs2) # 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!
```

9. Reboot the switch and verify that the running configuration is correct:

reload

```
(cs2) \# reload

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

System will now restart!
```

Configure the cluster switch log collection feature

The cluster switch health monitor log collection feature is used to collect switch-related log files in ONTAP. You must make sure that you have set up your environment using the BES-53248 cluster switch CLI as detailed here.

Steps

1. Generate the SSH keys:

crypto key generate

```
(switch) # show ip ssh
SSH Configuration
Administrative Mode: ..... Disabled
SSH Port: ..... 22
Protocol Level: ...... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA (521)
Key Generation In Progress: ..... None
SCP server Administrative Mode: ..... Disabled
(switch) # config
(switch) (Config) # crypto key generate rsa
Do you want to overwrite the existing RSA keys? (y/n): y
(switch) (Config) # crypto key generate dsa
Do you want to overwrite the existing DSA keys? (y/n): y
(switch) (Config) # crypto key generate ecdsa 521
Do you want to overwrite the existing ECDSA keys? (y/n): y
(switch) (Config) # aaa authorization commands "noCmdAuthList" none
(switch) (Config) # exit
(switch) # ip ssh server enable
(switch) # ip ssh pubkey-auth
(switch) # ip scp server enable
(switch) # write mem
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!
(switch) #
```

2. Verify that SSH is enabled:

show ip ssh

```
(switch) # show ip sshSSH ConfigurationEnabledAdministrative Mode:EnabledSSH Port:22Protocol Level:Version 2SSH Sessions Currently Active:0Max SSH Sessions Allowed:5SSH Timeout (mins):5Keys Present:DSA(1024) RSA(1024)ECDSA(521)Key Generation In Progress:NoneSCP server Administrative Mode:Disabled(switch) #
```

3. For ONTAP 9.8 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

system switch ethernet log setup-password system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```

4. For ONTAP 9.5P15, 9.6P11, 9.7P8 and later patch releases, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

system cluster-switch log setup-password system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the Cluster Switch Health Monitor (CSHM) configuration file

You can use this procedure to install the applicable configuration file for cluster switch health monitoring of BES-53248 cluster switches. In ONTAP releases 9.5P7 and earlier and 9.6P2 and earlier, you must download the cluster switch health monitor configuration file separately. In ONTAP releases 9.5P8 and later, 9.6P3 and later, and 9.7 and later, the cluster switch health monitor configuration file is bundled with ONTAP.

What you'll need

Before you setup the switch health monitor for BES-53248 cluster switches, you must ensure that the ONTAP cluster is up and running.



It is advisable to enable SSH in order to use all features available in CSHM.

Steps

- 1. Download the cluster switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the page: NetApp Software download
 - a. On the Software download page, select Switch Health Monitor Configuration Files
 - b. Select Platform = **ONTAP** and click **Go!**
 - c. On the Switch Health Monitor Configuration Files for ONTAP page, click View & Download
 - d. On the Switch Health Monitor Configuration Files for ONTAP Description page, click **Download** for the applicable cluster switch model, for example: **Broadcom-supported BES-53248**
 - e. On the End User License Agreement page, click Accept
 - f. On the Switch Health Monitor Configuration Files for ONTAP Download page, select the applicable configuration file, for example, **Broadcom_BES-53248.zip**
- 2. Upload the applicable zip file to your internal web server where the IP address is X.X.X.X.

For an internal web server IP address of 192.168.2.20 and assuming a /usr/download directory exists, you can upload your zip file to your web server using scp:

```
% scp Broadcom_BES-53248.zip
admin@192.168.2.20:/usr/download/Broadcom_BES-53248.zip
```

3. Access the advanced mode setting from one of the ONTAP systems in the cluster, using the command set -privilege advanced:

```
cluster1::> set -privilege advanced
```

4. Run the switch health monitor configure command system cluster-switch configure-health-monitor -node * -package-url http://server/file-location:

```
cluster1::> system cluster-switch configure-health-monitor -node *
-package-url
http://192.168.2.20/usr/download/Broadcom_BES-53248.zip
```

- Verify that the command output contains the text string "downloaded package processed successfully". If an error occurs, contact NetApp support.
- 6. Run the command system cluster-switch show on the ONTAP system and ensure that the cluster switches are discovered with the monitored field set to "True".

cluster1::> system cluster-switch show



If at any time you revert to an earlier version of ONTAP, you will need to install the CSHM configuration file again to enable switch health monitoring of BES-53248 cluster switches.

Verify the configuration after a cluster switch upgrade - BES-53248 switches

You can use the commands provided here to verify that all is operational after a BES-53248 cluster switch upgrade.

Steps

1. Display information about the network ports on the cluster using the command:

```
network port show -ipspace Cluster
```

Link must have the value up and Health Status must be healthy.

The following example shows the output from the command:

cluste	r1::> network	port show	-ipspa	ce Cli	uster		
Node:	node1						
Ignore						Crood (Mbra)	IIo al + b
Health						Speed (Mbps)	nealth
	IPspace					_	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node:							
Ignore						Speed (Mbps)	Health
Health Port Status	IPspace					Admin/Oper	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healthy
4	entries were	displayed.					

2. Verify that for each LIF Is Home is true and Status Admin/Oper is up on both nodes using the command:

network interface show -vserver Cluster

cluster1::>	network in	terface show	w -vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
	_				
Cluster					
	node1_clus	l up/up	169.254.217.125/16	node1	e0a
true					
	nodel_clus	2 up/up	169.254.205.88/16	node1	e0b
true					
	node2_clus	l up/up	169.254.252.125/16	node2	e0a
true		_			
	node2_clus2	2 up/up	169.254.110.131/16	node2	e0b
true					
4 entries we	ere displaye	ed.			

3. Verify that the Health Status of each node is true using the command: cluster show

Replace a Broadcom-supported BES-53248 cluster switch - BES-53248 switches

Replacing a defective Broadcom-supported BES-53248 cluster switch in a cluster network is a nondisruptive procedure (NDU).

What you'll need

The following conditions must exist before performing the switch replacement in the current environment and on the replacement switch.

- Existing cluster and network infrastructure:
 - The existing cluster must be verified as completely functional, with at least one fully connected cluster switch.

- All cluster ports must be up.
- All cluster logical interfaces (LIFs) must be administratively and operationally up and on their home ports.
- The ONTAP cluster ping-cluster -node node1 command must indicate that basic connectivity and larger than PMTU communication are successful on all paths.
- BES-53248 replacement cluster switch:
 - Management network connectivity on the replacement switch must be functional.
 - · Console access to the replacement switch must be in place.
 - The node connections are ports 0/1 through 0/16 with default licensing.
 - All Inter-Switch Link (ISL) ports must be disabled on ports 0/55 and 0/56.
 - The desired reference configuration file (RCF) and EFOS operating system switch image must be loaded onto the switch.
 - Initial customization of the switch must be complete, as detailed in Configuring a new Broadcomsupported BES-53248 switch.

Any previous site customizations, such as STP, SNMP, and SSH, should be copied to the new switch.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The names of the existing BES-53248 switches are cs1 and cs2.
- The name of the new BES-53248 switch is newcs2.
- The node names are node1 and node2.
- The cluster ports on each node are named e0a and e0b.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The prompt for changes to all cluster nodes is cluster1::>



The following procedure is based on the following cluster network topology:

```
Cluster1::> network port show -ipspace Cluster

Node: node1

Ignore
Speed(Mbps) Health

Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
-----
e0a Cluster Cluster up 9000 auto/10000 healthy
false
```

e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
Node: node	e2						
Ignore						Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU		
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healthy
4 entries	were display	ed.					
cluster1:	:> network in		w -vsei Netwoi		Cluste	er Current	Current
Is Vserver Home	Interface	Admin/Oper	Addres	ss/Mas	sk	Node	Port
Cluster	nodel clus	1 up/up	160 21	54 200	a 60/1	l6 node1	e0a
true	_		109.2	J4 • Z U .	9.09/1	io nodei	eva
true	node1_clus	2 up/up	169.25	54.49	.125/1	l6 node1	e0b
.	node2_clus	1 up/up	169.25	54.47	.194/1	l6 node2	e0a
true	node2_clus	2 up/up	169.25	54.19	.183/1	l6 node2	e0b
	were display	ed.					
Node/	cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platform						Platform

node2	-	_			0.40	
		cs1			0/2	BES-53248
node1	e0b /cdp	cs2			0/2	BES-53248
110001	_	cs1			0/1	BES-53248
		cs2			0/1	BES-53248
4 entries	s were di	splayed	1.			
(cs1) # s	show isdp	neighb	oors			
Capabilit	ty Codes:				lge, B - Sou IGMP, r - R	rce Route Bridge, epeater
Device II Port ID)		Intf	Holdtime	Capability	Platform
	-		0 / 1	175		DN 00750
node1 e0a			0/1	175	Н	FAS2750
node2			0/2	152	Н	FAS2750
e0a						
cs2			0/55	179	R	BES-53248
0/55						
cs2 0/56			0/56	179	R	BES-53248
(cs2) # s	show isdp	neighb	oors			
Capabilit	ty Codes:			- Trans Brid	lge, B - Sou	rce Route Bridge,
		5 - 5W	/ILCn, H -	- Host, I -	IGMP, r - R	epeater
Device II)	S - SW			IGMP, r - R Capability	
Port ID			Intf	Holdtime	Capability	Platform
Port ID node1						
Port ID node1 e0b			Intf 0/1	Holdtime 	Capability	PlatformFAS2750
Port ID node1 e0b node2			Intf	Holdtime	Capability	Platform
Port ID node1 e0b node2 e0b			Intf 0/1	Holdtime	Capability	PlatformFAS2750
Port ID			Intf 0/1 0/2	Holdtime	Capability H	Platform FAS2750 FAS2750
Port ID node1 e0b node2 e0b cs1			Intf 0/1 0/2	Holdtime 129 165 179	Capability H H	Platform FAS2750 FAS2750

Steps

1. Install the appropriate RCF and image on the switch, newcs2, and make any necessary site preparations.

If necessary, verify, download, and install the appropriate versions of the RCF and EFOS software for the new switch. If you have verified that the new switch is correctly set up and does not need updates to the RCF and EFOS software, continue to step 2.

- a. You can download the applicable Broadcom EFOS software for your cluster switches from the Broadcom Ethernet Switch Support site. Follow the steps on the Download page to download the EFOS file for the version of ONTAP software you are installing.
- b. The appropriate RCF is available from the Broadcom Cluster Switches page. Follow the steps on the Download page to download the correct RCF for the version of ONTAP software you are installing.
- 2. On the new switch, log in as admin and shut down all of the ports that will be connected to the node cluster interfaces (ports 1 to 16).



If you purchased additional licenses for additional ports, shut down these ports too.

If the switch that you are replacing is not functional and is powered down, the LIFs on the cluster nodes should have already failed over to the other cluster port for each node.



No password is required to enter enable mode.

```
User: admin
Password:
(newcs2) >enable
(newcs2) #config
(newcs2) (config) #interface 0/1-0/16
(newcs2) (interface 0/1-0/16) #shutdown
(newcs2) (interface 0/1-0/16) #exit
(newcs2) (config) #exit
```

3. Verify that all cluster LIFs have auto-revert enabled:

network interface show -vserver Cluster -fields auto-revert

4. Shut down the ISL ports 0/55 and 0/56 on the BES-53248 switch cs1:

```
(cs1) # config
(cs1) (config) # interface 0/55-0/56
(cs1) (interface 0/55-0/56) # shutdown
```

- 5. Remove all cables from the BES-53248 cs2 switch, and then connect them to the same ports on the BES-53248 newcs2 switch.
- 6. Bring up the ISLs ports 0/55 and 0/56 between the cs1 and newcs2 switches, and then verify the port channel operation status.

The Link State for port-channel 1/1 should be up and all member ports should be True under the Port Active heading.

This example enables ISL ports 0/55 and 0/56 and displays the Link State for port-channel 1/1 on switch cs1:

```
(cs1) # config
(cs1)(config) # interface 0/55-0/56
(cs1) (interface 0/55-0/56) # no shutdown
(cs1) # show port-channel 1/1
Channel Name...... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr Device/
            Port
                   Port
Ports Timeout
            Speed
                  Active
_____ ____
0/55 actor/long
            100G Full True
   partner/long
0/56 actor/long
            100G Full True
    partner/long
```

7. On the new switch newcs2, re-enable all of the ports that are connected to the node cluster interfaces (ports 1 to 16).



If you purchased additional licenses for additional ports, shut down these ports too.

```
User:admin
Password:
(newcs2) >enable
(newcs2) #config
(newcs2) (config) #interface 0/1-0/16
(newcs2) (interface 0/1-0/16) #no shutdown
(newcs2) (interface 0/1-0/16) #exit
(newcs2) (config) #exit
```

8. Verify that port e0b is up:

```
network port show -ipspace Cluster
```

The output should be similar to the following:

cluster1:	:> network po	rt show -ip	space (Cluste	er		
Node: node	e1						
Ignore						Speed(Mbps)	Hoolth
Health						speed (Mbps)	пеатип
	IPspace					_	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: node	e2						
Ignore						Speed(Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/auto	-
4 entries	were display	ed.					

9. On the same node as you used in the previous step, wait for the cluster LIF node1_clus2 on node1 to autorevert.

In this example, LIF node1_clus2 on node1 is successfully reverted if Is Home is true and the port is e0b.

The following command displays information about the LIFs on both nodes. Bringing up the first node is successful if Is Home is true for both cluster interfaces and they show the correct port assignments, in this example e0a and e0b on node1.

cluster::>	network inter	face show -	vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true	1 0 1 1	,	160 054 45 104/16	1 0	0
±	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true	node2_clus2	up/up	169.254.19.183/16	node2	e0a
false					
4 entries w	ere displayed				

10. Display information about the nodes in a cluster: cluster show

This example shows that the node health for node1 and node2 in this cluster is true:

11. Confirm the following cluster network configuration:

network port show

e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
Node: nod	e2						
Ignore				Spee	d (Mbp:	3)	Health
Health Port Status	IPspace	Broadcast	Domain				
 e0a	Cluster	Cluster			9000	auto/10000	healthy
false e0b	Cluster			-		auto/10000	-
false							
4 entries	were displa	yed.					
cluster1:	:> network i	nterface sho	ow -vse	rver	Cluste	er	
Current I	_	Status	Netwo	rk		Current	
Vserver Home		Admin/Oper	Addre	ss/Ma	sk	Node	Port
Cluster	node1_clu	s1 up/up	169.2	54.20	9.69/	16 node1	e0a
true	node1_clu	s2 up/up	169.2	54.49	.125/	16 node1	e0b
true	node2_clu	s1 up/up	169.2	54.47	.194/	16 node2	e0a
true	node2_clu	s2 up/up	169.2	54.19	.183/	16 node2	e0b
true 4 entries	were displa	yed.					
cs1# show	cdp neighbo	rs					
	y Codes: R -		_		_		

	/ - VoIP-Phone,			5	201200,	
S	s - Supports-STF	-Dispute				
Device-ID Port ID	Local Intrfce	Hldtme	Capab	ility	Platform	
node1	Eth1/1	144	Н		FAS2980	e0a
node2	Eth1/2	145	H		FAS2980	e0a
newcs2 (FDO296348FU) Eth1/65	·	176		S	N9K-C92300YC	
newcs2(FDO296348FU) Eth1/66	Eth1/66	176	R S I	S	N9K-C92300YC	!
Total entries displ	2520d • 1					
iocai encires dispi	Layeu. 4					
cs2# show cdp neigh						
cs2# show cdp neigh Capability Codes: F	nbors	Host, I D - Remo	- IGMP	, r - :	Repeater,	idge
cs2# show cdp neigh Capability Codes: F	nbors R - Router, T - S - Switch, H - 7 - VoIP-Phone,	Host, I D - Remo -Dispute	- IGMP	, r - i	Repeater, -Device,	idge Port
cs2# show cdp neigh Capability Codes: F S N S Device-ID ID	nbors R - Router, T - S - Switch, H - 7 - VoIP-Phone, S - Supports-STE Local Intrfce	Host, I D - Remo -Dispute	- IGMP tely-Ma	, r - : anaged ity P	Repeater, -Device,	
cs2# show cdp neigh Capability Codes: F S Device-ID ID node1	nbors R - Router, T - B - Switch, H - 7 - VoIP-Phone, B - Supports-STE Local Intrfce Eth1/1	Host, I D - Remo -Dispute Hldtme C	- IGMP tely-Ma	, r - : anaged ity P	Repeater, -Device, latform AS2980	Port
cs2# show cdp neigh Capability Codes: F S Device-ID ID node1	nbors R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STF Local Intrfce Eth1/1 Eth1/2	Host, I D - Remo -Dispute Hldtme C 139 H 124 H	- IGMP tely-Ma	, r - : anaged ity P F. F.	Repeater, -Device, latform AS2980	Port e0b

Total entries displayed: 4

12. Verify that the cluster network is healthy:

show isdp neighbors

(cs1)# show isdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater Device ID Intf Capability Holdtime Platform Port ID _____ ----_____ ----------_____ node1 0/1 175 Н FAS2750 e0a node2 0/2 152 Н FAS2750 e0a newcs2 0/55 179 R BES-53248 0/55 newcs2 0/56 179 R BES-53248 0/56 (newcs2) # show isdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater Device ID Intf Holdtime Capability Platform Port ID _____ -------------------_____ node1 0/1 129 Η FAS2750 e0b node2 0/2 165 Η FAS2750 e0b cs1 0/55 R BES-53248 0/55 179 0/56 179 R BES-53248 0/56 cs1

See Configuring the cluster switch log collection feature for the steps required to enable cluster health switch log collection used for collecting switch-related log files.

Related information

NetApp Support Site

NetApp Hardware Universe

Switch Setup and Configuration Guide for Broadcom-supported BES-53248 switches

Cisco Nexus 3132Q-V switches

Cisco Nexus 3132Q-V switches

You can use the Cisco Nexus 3132Q-V switches as cluster switches in your AFF or FAS cluster.

- You can install NX-OS and reference configuration files (RCFs) on the Cisco Nexus 3132Q-V cluster switch.
- You can migrate from a two-node switchless cluster environment to a two-node switched environment using Cisco Nexus 3132Q-V cluster switches.
- You can replace a defective Cisco Nexus 3132Q-V switch in a cluster and download the switch operating system and reference configuration file.
- You can replace Cisco Nexus 5596, Nexus 5020, or Nexus 5010 cluster switches with Cisco Nexus 3132Q-V switches.
- You can replace NetApp CN1610 switches with Cisco Nexus 3132Q-V cluster switches.

Available documentation

The following table lists the documentation available for the Cisco Nexus 3132Q-V switches.

Title	Description
Install a Cisco® Nexus 3132Q-V cluster switch and pass-through panel in a NetApp® cabinet	Describes how to install the pass-through panel in system cabinets where power connectors are at the front of the chassis and power distribution units are located in the rear of the chassis.
Setup the Cisco® Nexus 3132Q-V cluster switches	Describes how to setup and configure your Cisco Nexus 3132Q-V cluster switches.
Install NX-OS and Reference Configuration Files (RCFs)	Describes how to install NX-OS and reference configuration files (RCFs) on Nexus 3132Q-V cluster switch.
Replace Cisco Nexus 5596 cluster switches with Cisco Nexus 3132Q-V cluster switches	Describes how to migrate from environments that use older Cisco switches to environments that use Cisco 3132Q-V switches.
Replace CN1610 cluster switches with Cisco Nexus 3132Q-V cluster switches	Describes the procedure to replace a CN1610 switch with a Cisco Nexus 3132Q-V cluster switch.
Migrate from a two-node Switchless Cluster	Describes how to migrate from a two-node switchless cluster environment to a two-node switched environment using Cisco Nexus 3132Q-V cluster switches.

Describes the procedure to replace a defective Cisco Nexus 3132Q-V switch in a cluster and download the switch operating system and reference configuration file.

Install a Cisco Nexus 3132Q-V cluster switch and a passthrough panel in a NetApp cabinet

You can install the Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.

Before you begin

You must have reviewed the initial preparation requirements, kit contents, and safety precautions.

Cisco Nexus 3000 Series Hardware Installation Guide

About this task

- For each switch, you must supply the eight 10-32 or 12-24 screws and clip nuts to mount the brackets and slider rails to the front and rear cabinet posts.
- You must use the Cisco standard rail kit to install the switch in a NetApp cabinet.



The jumper cords are not included with the pass-through kit and should be included with your switches. If they were not shipped with the switches, you can order them from NetApp (part number X1558A-R6).

Steps

1. Install the pass-through blanking panel in the NetApp cabinet.

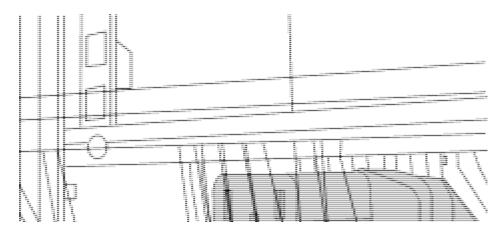
The pass-through panel kit is available from NetApp (part number X8784-R6).

The NetApp pass-through panel kit contains the following hardware:

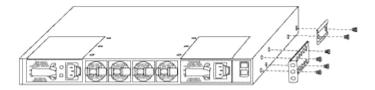
- One pass-through blanking panel
- Four 10-32 x .75 screws
- Four 10-32 clip nuts
 - a. Determine the vertical location of the switches and blanking panel in the cabinet.

In this procedure, the blanking panel will be installed in U40.

- b. Install two clip nuts on each side in the appropriate square holes for front cabinet rails.
- c. Center the panel vertically to prevent intrusion into adjacent rack space, and then tighten the screws.
- d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



- 1. Female connector of the jumper cord.
- 2. Install the rack-mount brackets on the Nexus 3132Q-V switch chassis.
 - a. Position a front rack-mount bracket on one side of the switch chassis so that the mounting ear is aligned with the chassis faceplate (on the PSU or fan side), and then use four M4 screws to attach the bracket to the chassis.



- b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.
- c. Install the rear rack-mount bracket on the switch chassis.
- d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.
- 3. Install the clip nuts in the square hole locations for all four IEA posts.



The two 3132Q-V switches will always be mounted in the top 2U of the cabinet RU41 and 42.

- 4. Install the slider rails in the cabinet.
 - a. Position the first slider rail at the RU42 mark on the back side of the rear left post, insert screws with the matching thread type, and then tighten the screws with your fingers.



- 1. As you gently slide the slider rail, align it to the screw holes in the rack.
- 2. Tighten the screws of the slider rails to the cabinet posts.
- b. Repeat step 4a for the right side rear post.

- c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.
- 5. Install the switch in the cabinet.



This step requires two people: one person to support the switch from the front and another to guide the switch into the rear slider rails.

a. Position the back of the switch at RU41.



- 1. As the chassis is pushed toward the rear posts, align the two rear rack-mount guides with the slider rails.
- 2. Gently slide the switch until the front rack-mount brackets are flush with the front posts.
- b. Attach the switch to the cabinet.



- 1. With one person holding the front of the chassis level, the other person should fully tighten the four rear screws to the cabinet posts.
- c. With the chassis now supported without assistance, fully tighten the front screws to the posts.
- d. Repeat steps 5a through 5c for the second switch at the RU42 location.



By using the fully installed switch as a support, it is not necessary to hold the front of the second switch during the installation process.

- 6. When the switches are installed, connect the jumper cords to the switch power inlets.
- 7. Connect the male plugs of both jumper cords to the closest available PDU outlets.



To maintain redundancy, the two cords must be connected to different PDUs.

8. Connect the management port on each 3132Q-V switch to either of the management switches (if ordered) or connect them directly to your management network.

The management port is the upper-right port located on the PSU side of the switch. The CAT6 cable for each switch needs to be routed through the pass-through panel after the switches are installed to connect to the management switches or management network.

Set up

Set up the switches

If you do not already have the required configuration information and documentation, you need to gather that information before setting up your cluster and management network switches.

- You must have access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- You must have the required cluster network and management network switch documentation.

See Required documentation for more information.

• You must have the required controller documentation and ONTAP documentation.

NetApp documentation

- You must have the applicable licenses, network and configuration information, and cables.
- You must have the completed cabling worksheets.



Due to the complexity that can result from illustrating layers of cabling, this guide does not provide cabling graphics. This guide does provide sample worksheets with recommended port assignments and blank worksheets that you can use to set up your cluster.



For more information refer to the Hardware Universe.

 All Cisco cluster network and management network switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software but do not have the RCFs loaded.



You must download the applicable NetApp cluster network and management network RCFs from the NetApp Support Site at mysupport.netapp.com for the switches that you receive.

 In addition, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for the 92300YC cluster switches. See Installing the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches for details.

Steps

1. Rack the cluster network and management network switches and controllers.

If you are installing your	Then
Cisco Nexus 9336C-FX2 in a NetApp system cabinet	See the <i>Installing a Cisco Nexus</i> 9336C-FX2 cluster switch and pass-through panel in a NetApp cabinet guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3232C in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.
Cisco Nexus 5596UP/5596T in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 5596 cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.

- 2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheets.
- 3. Power on the cluster network and management network switches and controllers.
- Perform an initial configuration of the cluster network switches based on information provided in Required configuration information.
- 5. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
- 6. Check the version on the cluster network switches, and if necessary, download the NetApp-supported version of the software to the switches.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Cluster Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and the instructions from the Cisco Ethernet Switches page.

7. Check the software version on the network switches and, if necessary, download the NetApp-supported version of the software to the switches. If you have your own switches, refer to the Cisco site.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Management Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and instructions from the Cisco Ethernet Switches page.

Related information

Required cluster configuration information

Required documentation

Sample and blank cabling worksheets

Required cluster configuration information

To configure your cluster, you need the appropriate number and type of cables and cable connectors for your switches. Depending on the type of switch you are initially configuring, you need to connect to the switch console port with the included console cable; you also need to provide specific network information.

Required network information for all switches

You need the following network information for all switch configurations:

- · IP subnet for management network traffic
- · Host names and IP addresses for each of the storage system controllers and all applicable switches
- Most storage system controllers are managed through the e0M interface by connecting to the Ethernet service port (wrench icon). On AFF A800 and AFF A700 systems, the e0M interface uses a dedicated Ethernet port.

Refer to the Hardware Universe for latest information.

Required network information for Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches

For the Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches, you need to provide applicable responses to the following initial setup questions when you first boot the switch. Your site's security policy defines the responses and services to enable.

Abort Auto Provisioning and continue with normal setup? (yes/no)

Respond with yes. The default is no.

• Do you want to enforce secure password standard? (yes/no)

Respond with **yes**. The default is yes.

• Enter the password for admin:

The default password is "admin"; you must create a new, strong password. A weak password can be rejected.

Would you like to enter the basic configuration dialog? (yes/no)

Respond with **yes** at the initial configuration of the switch.

Create another login account? (yes/no)

Your answer depends on your site's policies on alternate administrators. The default is no.

Configure read-only SNMP community string? (yes/no)

Respond with **no**. The default is no.

• Configure read-write SNMP community string? (yes/no)

Respond with **no**. The default is no.

• Enter the switch name.

The switch name is limited to 63 alphanumeric characters.

• Continue with Out-of-band (mgmt0) management configuration? (yes/no)

Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip address.

Configure the default-gateway? (yes/no)

Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.

Configure advanced IP options? (yes/no)

Respond with **no**. The default is no.

• Enable the telnet service? (yes/no)

Respond with **no**. The default is no.

• Enabled SSH service? (yes/no)

Respond with **yes**. The default is yes.



SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.

- Enter the type of SSH key you want to generate (dsa/rsa/rsa1). The default is rsa.
- Enter the number of key bits (1024-2048).
- Configure the NTP server? (yes/no)

Respond with **no**. The default is no.

• Configure default interface layer (L3/L2):

Respond with **L2**. The default is L2.

Configure default switch port interface state (shut/noshut):

Respond with **noshut**. The default is noshut.

• Configure CoPP system profile (strict/moderate/lenient/dense):

Respond with **strict**. The default is strict.

• Would you like to edit the configuration? (yes/no)

You should see the new configuration at this point. Review and make any necessary changes to the

configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.

• Use this configuration and save it? (yes/no)

Respond with **yes** to save the configuration. This automatically updates the kickstart and system images.



If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

For more information about the initial configuration of your switch, see the following guides:

Cisco Nexus 9336C-FX2 Installation and Upgrade Guides

Cisco Nexus 92300YC Installation and Upgrade Guides

Cisco Nexus 5000 Series Hardware Installation Guide

Cisco Nexus 3000 Series Hardware Installation Guide

Install the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches

You can use this procedure to install the applicable configuration file for cluster switch health monitoring of Nexus 92300YC cluster switches. In ONTAP releases 9.5P7 and earlier and 9.6P2 and earlier, you must download the cluster switch health monitor configuration file separately. In ONTAP releases 9.5P8 and later, 9.6P3 and later, and 9.7 and later, the cluster switch health monitor configuration file is bundled with ONTAP.

Before you setup the switch health monitor for 92300YC cluster switches, you must ensure that the ONTAP cluster is up and running.



It is advisable to enable SSH in order to use all features available in CSHM.

- 1. Download the cluster switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the NetApp Software download page.
 - a. On the Software download page, select Switch Health Monitor Configuration Files
 - b. Select Platform = **ONTAP** and click **Go!**
 - c. On the Switch Health Monitor Configuration Files for ONTAP page, click View & Download
 - d. On the Switch Health Monitor Configuration Files for ONTAP Description page, click **Download** for the applicable cluster switch model, for example: **Cisco Nexus 92300YC**
 - e. On the End User License Agreement page, click Accept
 - f. On the Switch Health Monitor Configuration Files for ONTAP Download page, select the applicable configuration file, for example, Cisco_Nexus_92300YC.zip
- 2. Upload the applicable zip file to your internal web server where the IP address is X.X.X.X.

For an internal web server IP address of 192.168.2.20 and assuming a /usr/download directory exists, you can upload your zip file to your web server using scp:

```
% scp Cisco_Nexus_92300YC.zip
admin@192.168.2.20:/usr/download/Cisco_Nexus_92300YC.zip
```

3. Access the advanced mode setting from one of the ONTAP systems in the cluster, using the command setprivilege advanced:

```
cluster1::> set -privilege advanced
```

4. Run the switch health monitor configure command system cluster-switch configure-health-monitor -node * -package-url X.X.X.X/location_to_download_zip_file:

```
cluster1::> system cluster-switch configure-health-monitor -node *
-package-url 192.168.2.20/usr/download/Cisco_Nexus_92300YC.zip
```

- 5. Verify that the command output contains the text string "downloaded package processed successfully". If an error occurs, contact NetApp support.
- 6. Run the command system cluster-switch show on the ONTAP system and ensure that the cluster switches are discovered with the monitored field set to "True".

```
cluster1::> system cluster-switch show
```



If at any time you revert to an earlier version of ONTAP, you will need to install the CSHM configuration file again to enable switch health monitoring of 92300YC cluster switches.

Required documentation

You need specific switch and controller documentation to set up your ONTAP cluster.

Required documentation for cluster network switches

To set up the Cisco Nexus 9336C-FX2 and 92300YC switches, you need the following documentation from the Cisco Nexus 9000 Series Switches Support page:

Document title	Description
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.

Document title	Description
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

To set up the Cisco Nexus 3232C and 3132Q-V switches, you need the following documentation from the Cisco Nexus 3000 Series Switches Support page:

Document title	Description
Nexus 3000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 3000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 3000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.

Document title	Description
Cisco Nexus 3000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.
Nexus 3000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 3000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 3000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 3000 series switches.

To set up the Cisco Nexus 5596 switch, you need the following documents from Cisco Nexus 5000 Series Switches Support page:

Document title	Description
Nexus 5000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 5000 Series Switch Software Configuration Guide (choose the guide for the software you are using)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide	Provides information about how to downgrade the switch to the supported ONTAP switch software, if necessary.
Cisco Nexus 5000 Series NX-OS Command Reference Master Index	Provides an alphabetical list of all the commands supported for a specific NX-OS release.
Cisco Nexus 5000 and Nexus 2000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 5000 switches.
Nexus 5000 Series NX-OS System Message Reference	Describes troubleshooting information.

Document title	Description
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000 Series, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 5000 series switches.

Required documentation for supported ONTAP systems

To set up an ONTAP system, you need the following documents for your version of the operating system from the ONTAP 9 Documentation Center.

Name	Description
Controller-specific Installation and Setup Instructions	Describes how to install NetApp hardware.
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.
Hardware Universe	Provides NetApp hardware configuration and compatibility information.

Rail kit and cabinet documentation

To install a Cisco switch in a NetApp cabinet, see the following hardware documentation:

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet	Describes how to install a Cisco Nexus 3232C switch in a four-post NetApp cabinet.
Installing a Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 3132Q-V switch in a four-post NetApp cabinet.
Installing a Cisco Nexus 5596 switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 5596 switch in a NetApp cabinet.

Considerations for using Smart Call Home

Smart Call Home monitors the hardware and software components on your network, to generate an email-based notification of critical system conditions. When an event occurs on your device, Smart Call Home raises an alert to all the recipients that are configured in your destination profile.

You must configure a cluster network switch to communicate using email with the Smart Call Home system. You can optionally set up your cluster network switch to take advantage of Cisco's embedded Smart Call Home support feature.

Before you can use Smart Call Home feature, you need to be aware of the following considerations:

- An email server must be in place.
- The switch must have IP connectivity to the email server.
- The contact name (SNMP server contact), phone number, and street address information must be configured.
- This is required to determine the origin of messages received.
- A CCO ID must be associated with an appropriate Cisco SMARTnet Service contract for your company.
- Cisco SMARTnet Service must be in place for the device to be registered.

The Cisco support site contains information about the commands to configure Smart Call Home.

Cisco support site

Sample and blank cabling worksheets

The sample cabling worksheets provide examples of recommended port assignments from the switches to the controllers. The blank worksheets provide a template that you can use in setting up your cluster.

Cisco Nexus 9336C-FX2 cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10GbE node 1	1	4x10GbE node 1
2	4x10GbE node 2	2	4x10GbE node 2
3	4x10GbE node 3	3	4x10GbE node 3
4	4x25GbE node 4	4	4x25GbE node 4
5	4x25GbE node 5	5	4x25GbE node 5
6	4x25GbE node 6	6	4x25GbE node 6

Cluster switch A		Cluster switch B	
7	4x100GbE node 7	7	4x100GbE node 7
8	4x100GbE node 8	8	4x100GbE node 8
9	4x100GbE node 9	9	4x100GbE node 9
10	4x100GbE node 10	10	4x100GbE node 10
11	4x100GbE node 11	11	4x100GbE node 11
12	4x100GbE node 12	12	4x100GbE node 12
13	4x100GbE node 13	13	4x100GbE node 13
14	4x100GbE node 14	14	4x100GbE node 14
15	4x100GbE node 15	15	4x100GbE node 15
16	4x100GbE node 16	16	4x100GbE node 16
17	4x100GbE node 17	17	4x100GbE node 17
18	4x100GbE node 18	18	4x100GbE node 18
19	4x100GbE node 19	19	4x100GbE node 19
20	4x100GbE node 20	20	4x100GbE node 20
21	4x100GbE node 21	21	4x100GbE node 21
22	4x100GbE node 22	22	4x100GbE node 22
23	4x100GbE node 23	23	4x100GbE node 23
24	4x100GbE node 24	24	4x100GbE node 24
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A	Cluster switch B	
1	1	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	
11	11	
12	12	
13	13	
14	14	
15	15	
16	16	
17	17	
18	18	
19	19	

Cluster switch A		Cluster switch B	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Cisco Nexus 92300YC cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	10/25 GbE node	1	10/25 GbE node
2	10/25 GbE node	2	10/25 GbE node
3	10/25 GbE node	3	10/25 GbE node
4	10/25 GbE node	4	10/25 GbE node
5	10/25 GbE node	5	10/25 GbE node
6	10/25 GbE node	6	10/25 GbE node
7	10/25 GbE node	7	10/25 GbE node

Cluster switch A		Cluster switch	Cluster switch B	
8	10/25 GbE node	8	10/25 GbE node	
9	10/25 GbE node	9	10/25 GbE node	
10	10/25 GbE node	10	10/25 GbE node	
11	10/25 GbE node	11	10/25 GbE node	
12	10/25 GbE node	12	10/25 GbE node	
13	10/25 GbE node	13	10/25 GbE node	
14	10/25 GbE node	14	10/25 GbE node	
15	10/25 GbE node	15	10/25 GbE node	
16	10/25 GbE node	16	10/25 GbE node	
17	10/25 GbE node	17	10/25 GbE node	
18	10/25 GbE node	18	10/25 GbE node	
19	10/25 GbE node	19	10/25 GbE node	
20	10/25 GbE node	20	10/25 GbE node	
21	10/25 GbE node	21	10/25 GbE node	
22	10/25 GbE node	22	10/25 GbE node	
23	10/25 GbE node	23	10/25 GbE node	
24	10/25 GbE node	24	10/25 GbE node	
25	10/25 GbE node	25	10/25 GbE node	
26	10/25 GbE node	26	10/25 GbE node	
27	10/25 GbE node	27	10/25 GbE node	
28	10/25 GbE node	28	10/25 GbE node	
29	10/25 GbE node	29	10/25 GbE node	

Cluster switch A		Cluster switch E	Cluster switch B	
30	10/25 GbE node	30	10/25 GbE node	
31	10/25 GbE node	31	10/25 GbE node	
32	10/25 GbE node	32	10/25 GbE node	
33	10/25 GbE node	33	10/25 GbE node	
34	10/25 GbE node	34	10/25 GbE node	
35	10/25 GbE node	35	10/25 GbE node	
36	10/25 GbE node	36	10/25 GbE node	
37	10/25 GbE node	37	10/25 GbE node	
38	10/25 GbE node	38	10/25 GbE node	
39	10/25 GbE node	39	10/25 GbE node	
40	10/25 GbE node	40	10/25 GbE node	
41	10/25 GbE node	41	10/25 GbE node	
42	10/25 GbE node	42	10/25 GbE node	
43	10/25 GbE node	43	10/25 GbE node	
44	10/25 GbE node	44	10/25 GbE node	
45	10/25 GbE node	45	10/25 GbE node	
46	10/25 GbE node	46	10/25 GbE node	
47	10/25 GbE node	47	10/25 GbE node	
48	10/25 GbE node	48	10/25 GbE node	
49	40/100 GbE node	49	40/100 GbE node	
50	40/100 GbE node	50	40/100 GbE node	
51	40/100 GbE node	51	40/100 GbE node	

Cluster switch A		Cluster switch B	
52	40/100 GbE node	52	40/100 GbE node
53	40/100 GbE node	53	40/100 GbE node
54	40/100 GbE node	54	40/100 GbE node
55	40/100 GbE node	55	40/100 GbE node
56	40/100 GbE node	56	40/100 GbE node
57	40/100 GbE node	57	40/100 GbE node
58	40/100 GbE node	58	40/100 GbE node
59	40/100 GbE node	59	40/100 GbE node
60	40/100 GbE node	60	40/100 GbE node
61	40/100 GbE node	61	40/100 GbE node
62	40/100 GbE node	62	40/100 GbE node
63	40/100 GbE node	63	40/100 GbE node
64	40/100 GbE node	64	40/100 GbE node
65	100 GbE ISL to switch B port 65	65	100 GbE ISL to switch A port 65
66	100 GbE ISL to switch B port 66	66	100 GbE ISL to switch A port 65

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	

Cluster switch A	Cluster switch B	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	
11	11	
12	12	
13	13	
14	14	
15	15	
16	16	
17	17	
18	18	
19	19	
20	20	
21	21	
22	22	
23	23	
24	24	

Cluster switch A	Cluster switch B	
25	25	
26	26	
27	27	
28	28	
29	29	
30	30	
31	31	
32	32	
33	33	
34	34	
35	35	
36	36	
37	37	
38	38	
39	39	
40	40	
41	41	
42	42	
43	43	
44	44	
45	45	
46	46	

Cluster switch A		Cluster switch B	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL to switch B port 65	65	ISL to switch A port 65
66	ISL to switch B port 66	66	ISL to switch A port 66

Cisco Nexus 3232C cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling

worksheet by using the completed sample cabling worksheet as a guide. Each switch can be configured as a single 100GbE, 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G/100G node	1	4x10G/40G/100G node
2	4x10G/40G/100G node	2	4x10G/40G/100G node
3	4x10G/40G/100G node	3	4x10G/40G/100G node
4	4x10G/40G/100G node	4	4x10G/40G/100G node
5	4x10G/40G/100G node	5	4x10G/40G/100G node
6	4x10G/40G/100Gnode	6	4x10G/40G/100Gnode
7	4x10G/40G/100G node	7	4x10G/40G/100G node
8	4x10G/40G/100G node	8	4x10G/40G/100G node
9	4x10G/40G/100G node	9	4x10G/40G/100G node
10	4x10G/40G/100G node	10	4x10G/40G/100G node
11	4x10G/40G/100G node	11	4x10G/40G/100G node
12	4x10G/40G/100G node	12	4x10G/40G/100G node
13	4x10G/40G/100G node	13	4x10G/40G/100G node
14	4x10G/40G/100G node	14	4x10G/40G/100G node
15	4x10G/40G/100G node	15	4x10G/40G/100G node
16	4x10G/40G/100G node	16	4x10G/40G/100G node
17	4x10G/40G/100G node	17	4x10G/40G/100G node
18	4x10G/40G/100G node	18	4x10G/40G/100G node

Cluster switch A		Cluster switch B	
19	40G/100G node 19	19	40G/100G node 19
20	40G/100G node 20	20	40G/100G node 20
21	40G/100G node 21	21	40G/100G node 21
22	40G/100G node 22	22	40G/100G node 22
23	40G/100G node 23	23	40G/100G node 23
24	40G/100G node 24	24	40G/100G node 24
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	

Cluster switch A		Cluster switch B	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Cisco Nexus 3132Q-V cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide. Each switch can

be configured as a single 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G node	1	4x10G/40G node
2	4x10G/40G node	2	4x10G/40G node
3	4x10G/40G node	3	4x10G/40G node
4	4x10G/40G node	4	4x10G/40G node
5	4x10G/40G node	5	4x10G/40G node
6	4x10G/40G node	6	4x10G/40G node
7	4x10G/40G node	7	4x10G/40G node
8	4x10G/40G node	8	4x10G/40G node
9	4x10G/40G node	9	4x10G/40G node
10	4x10G/40G node	10	4x10G/40G node
11	4x10G/40G node	11	4x10G/40G node
12	4x10G/40G node	12	4x10G/40G node
13	4x10G/40G node	13	4x10G/40G node
14	4x10G/40G node	14	4x10G/40G node
15	4x10G/40G node	15	4x10G/40G node
16	4x10G/40G node	16	4x10G/40G node
17	4x10G/40G node	17	4x10G/40G node
18	4x10G/40G node	18	4x10G/40G node
19	40G node 19	19	40G node 19

Cluster switch A		Cluster switch B	
20	40G node 20	20	40G node 20
21	40G node 21	21	40G node 21
22	40G node 22	22	40G node 22
23	40G node 23	23	40G node 23
24	40G node 24	24	40G node 24
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B		
Switch port	Node/port usage	Switch port	Node/port usage	
1		1		
2		2		
3		3		
4		4		
5		5		
6		6		
7		7		
8		8		
9		9		

Cluster switch A		Cluster switch B		
10		10		
11		11		
12		12		
13		13		
14		14		
15		15		
16		16		
17		17		
18		18		
19		19		
20		20		
21		21		
22		22		
23		23		
24		24		
25 through 30	Reserved	25 through 30	Reserved	
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31	
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32	

Cisco Nexus 5596UP and 5596T cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

Some platforms support more than one 10GbE cluster port connection per cluster interconnect switch. To support additional cluster connections, you can use ports 25 through 40, as well as ports 49 through 80 when expansion modules are installed.

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	Node port 1	1	Node port 1
2	Node port 2	2	Node port 2
3	Node port 3	3	Node port 3
4	Node port 4	4	Node port 4
5	Node port 5	5	Node port 5
6	Node port 6	6	Node port 6
7	Node port 7	7	Node port 7
8	Node port 8	8	Node port 8
9	Node port 9	9	Node port 9
10	Node port 10	10	Node port 10
11	Node port 11	11	Node port 11
12	Node port 12	12	Node port 12
13	Node port 13	13	Node port 13
14	Node port 14	14	Node port 14
15	Node port 15	15	Node port 15
16	Node port 16	16	Node port 16
17	Node port 17	17	Node port 17
18	Node port 18	18	Node port 18

Cluster switch A		Cluster switch B		
19	Node port 19	19	Node port 19	
20	Node port 20	20	Node port 20	
21	Node port 21	21	Node port 21	
22	Node port 22	22	Node port 22	
23	Node port 23	23	Node port 23	
24	Node port 24	24	Node port 24	
25 through 40	Reserved	25 through 40	Reserved	
41	ISL to switch B port 41	41	ISL to switch A port 41	
42	ISL to switch B port 42	42	ISL to switch A port 42	
43	ISL to switch B port 43	43	ISL to switch A port 43	
44	ISL to switch B port 44	44	ISL to switch A port 44	
45	ISL to switch B port 45	45	ISL to switch A port 45	
46	ISL to switch B port 46	46	ISL to switch A port 46	
47	ISL to switch B port 47	47	ISL to switch A port 47	
48	ISL to switch B port 48	48	ISL to switch A port 48	

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.



Switch ports 1 through 24 function as 10 GbE ports. Switch ports 41 through 48 are reserved for Inter-Switch Links (ISLs).

Cluster switch A		Cluster switch B		
Switch port Node/port usage		Switch port Node/port usage		
1		1		

Cluster switch A	Cluster switch B	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	
11	11	
12	12	
13	13	
14	14	
15	15	
16	16	
17	17	
18	18	
19	19	
20	20	
21	21	
22	22	
23	23	

Cluster switch A		Cluster switch B	
24		24	
25 through 40	Reserved	25 through 40	Reserved
41	ISL to switch B port 41	41	ISL to switch A port 41
42	ISL to switch B port 42	42	ISL to switch A port 42
43	ISL to switch B port 43	43	ISL to switch A port 43
44	ISL to switch B port 44	44	ISL to switch A port 44
45	ISL to switch B port 45	45	ISL to switch A port 45
46	ISL to switch B port 46	46	ISL to switch A port 46
47	ISL to switch B port 47	47	ISL to switch A port 47
48	ISL to switch B port 48	48	ISL to switch A port 48

Install NX-OS software and RCFs on Cisco Nexus 3132Q-V cluster switches

The Cisco NX-OS software and reference configuration files (RCFs) must be installed on Cisco Nexus 3132Q-V cluster switches.

Before you begin

The following conditions must exist before you install the NX-OS software and Reference Configurations Files (RCFs) on the cluster switch:

- The cluster must be fully functioning (there should be no errors in the logs or similar issues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have a console connection to the switch, required when installing the RCF.
- You must have consulted the switch compatibility table on the Cisco Ethernet switch page for the supported ONTAP, NX-OS, and RCF versions.
- There can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on Cisco Nexus 3000 Series Switches.

· You must have the current RCF.

About this task

The examples in this procedure use two nodes. These nodes use two 10GbE cluster interconnect ports e0a and e0b.

See the Hardware Universe to verify the correct cluster ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are cluster1-01 and cluster1-02.
- The cluster LIF names are cluster1-01_clus1 and cluster1-01_clus2 for cluster1-01 and cluster1-02 clus1 and cluster1-02 clus2 for cluster1-02.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=x h
```

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

3. Display how many cluster interconnect interfaces are configured in each node for each cluster interconnect switch:

network device-discovery show -protocol cdp

cluster1::*	> netwo	rk device-discovery show -	protocol cdp	
		Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
cluster1-02	/cdp			
	e0a	cs1	Eth1/2	N3K-
C3132Q-V				
	e0b	cs2	Eth1/2	N3K-
C3132Q-V				
cluster1-01	/cdp			
	e0a	cs1	Eth1/1	N3K-
C3132Q-V				
	e0b	cs2	Eth1/1	N3K-
C3132Q-V				
4 entries w	ere dis	played.		

- 4. Check the administrative or operational status of each cluster interface.
 - a. Display the network port attributes:

network port show -ipspace Cluster

cluster1:	:*> network p	ort show -:	ipspace	Clust	ter		
Node: clus	ster1-02						
						Speed (Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
Node: clus	ster1-01						
						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
4 entries	were display	ed.					

b. Display information about the LIFs:

network interface show -vserver Cluster

cluster1::*	> network interface	show -vser	ver Cluster	
	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port Home	е			
Cluster				
	cluster1-01_clus1	up/up	169.254.209.69/16	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.49.125/16	
cluster1-01	eOb true			
	cluster1-02_clus1	up/up	169.254.47.194/16	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.19.183/16	
cluster1-02	e0b true			
4 entries we	ere displayed.			

5. Ping the remote cluster LIFs:

cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node cluster1-02
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01 clus1 169.254.209.69 cluster1-01
                                                           e0a
Cluster cluster1-01 clus2 169.254.49.125 cluster1-01
                                                           e0b
Cluster cluster1-02 clus1 169.254.47.194 cluster1-02
                                                           e0a
Cluster cluster1-02 clus2 169.254.19.183 cluster1-02
                                                           e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Verify that the auto-revert command is enabled on all cluster LIFs:

network interface show -vserver Cluster -fields auto-revert

7. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files by using the commands:

system switch ethernet log setup-password

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? \{y|n\}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y | n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

8. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files by using the commands:

```
system cluster-switch log setup-password
system cluster-switch log enable-collection
```

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y | n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 3132Q-V cluster switch.

Steps

1. Connect the cluster switch to the management network.

2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the NX-OS software to the Nexus 3132Q-V switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password: xxxxxxxx
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.4.bin /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Verify the running version of the NX-OS software:

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
but not
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
```

```
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 04.25
NXOS: version 9.3(3)
  BIOS compile time: 01/28/2020
 NXOS image file is: bootflash:///nxos.9.3.3.bin
                  NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:371
Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID F0xxxxxxx23
  Device name: cs2
  bootflash: 15137792 kB
  usb1:
                      0 kB (expansion flash)
Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
Last reset at 663500 usecs after Mon Nov 2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

5. Install the NX-OS image.

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS
Verifying image type.
[] 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS
Performing module support checks.
[] 100% -- SUCCESS
Notifying services about system upgrade.
[] 100% -- SUCCESS
Compatibility check is done:
Module bootable
                                     Install-type Reason
reset
        yes
                     disruptive
                                                 default
upgrade is not hitless
Images will be upgraded according to following table:
Module Image Running-Version(pri:alt)
                                                     New-
             Upg-Required
Version
______
_____
   1 nxos 9.3(3)
                                                      9.3(4)
yes
   1 bios v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020) 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.
```

```
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.

cs2#
```

6. Verify the new version of NX-OS software after the switch has rebooted:

show version

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
 BIOS: version 04.25
NXOS: version 9.3(4)
 BIOS compile time: 05/22/2019
  NXOS image file is: bootflash:///nxos.9.3.4.bin
```

```
NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]
Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23
  Device name: cs2
 bootflash: 15137792 kB
  usb1:
                      0 kB (expansion flash)
Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
Last reset at 663500 usecs after Mon Nov 2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 3132Q-V switch for the first time. You can also use this procedure to upgrade your RCF version.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are cluster1-01, cluster1-02, cluster1-03, and cluster1-04.
- The cluster LIF names are cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1, and cluster1-04_clus2.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches:

network device-discovery show

		Discovered		
		Device (LLDP: ChassisID)		Platform
cluster1-0	1/cdp			
	e0a	cs1	Ethernet1/7	N3K-
C3132Q-V				
	e0d	cs2	Ethernet1/7	N3K-
C3132Q-V				
cluster1-0	2/cdp			
	e0a	cs1	Ethernet1/8	N3K-
C3132Q-V				
	e0d	cs2	Ethernet1/8	N3K-
C3132Q-V				
cluster1-0	3/cdp			
	e0a	cs1	Ethernet1/1/1	N3K-
C3132Q-V				
	e0b	cs2	Ethernet1/1/1	N3K-
C3132Q-V				
cluster1-0	4/cdp			
	e0a	cs1	Ethernet1/1/2	N3K-
C3132Q-V				
	e0b	cs2	Ethernet1/1/2	N3K-
C3132Q-V				

- 2. Check the administrative and operational status of each cluster port.
 - a. Verify that all the cluster ports are up with a healthy status:

network port show -role cluster

```
Cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
```

e0a Cluster Cluster up 9000 auto/10 healthy false e0d Cluster Cluster up 9000 auto/10 healthy false	
healthy false e0d Cluster Cluster up 9000 auto/10	10000
healthy false e0d Cluster Cluster up 9000 auto/10	10000
_	
healthy false	0000
Node: cluster1-02	
Ignore	
Speed (Mk	ops) Health
Port IPspace Broadcast Domain Link MTU Admin/Op	per Status
Status	
e0a Cluster Cluster up 9000 auto/10	0000
healthy false	2000
e0d Cluster Cluster up 9000 auto/10 healthy false	70000
8 entries were displayed.	
Node: cluster1-03	
Node: elastell to	
Ignore)
Health Speed (MK	ops) Health
Port IPspace Broadcast Domain Link MTU Admin/Op	per Status
Status	
e0a Cluster Cluster up 9000 auto/10	0000 healthy
false)000 bool+br
false e0b Cluster Cluster up 9000 auto/10 false	0000 healthy
e0b Cluster Cluster up 9000 auto/10 false	0000 healthy
e0b Cluster Cluster up 9000 auto/10	0000 healthy
e0b Cluster Cluster up 9000 auto/10 false	0000 healthy
e0b Cluster Cluster up 9000 auto/10 false Node: cluster1-04 Ignore Speed (Mk	ops) Health
e0b Cluster Cluster up 9000 auto/10 false Node: cluster1-04 Ignore Speed(Mk	ops) Health
e0b Cluster Cluster up 9000 auto/10 false Node: cluster1-04 Ignore Speed (Mk	ops) Health
e0b Cluster Cluster up 9000 auto/10 false Node: cluster1-04 Ignore Speed (Mk Health Port IPspace Broadcast Domain Link MTU Admin/Op	ops) Health
e0b Cluster Cluster up 9000 auto/10 false Node: cluster1-04 Ignore Speed (Mk Health Port IPspace Broadcast Domain Link MTU Admin/Op	ops) Health oer Status

false								
e0b	Cluster	Cluster	up	9000	auto/10000	healthy		
false								
cluster1::*>								

b. Verify that all the cluster interfaces (LIFs) are on the home port:

network interface show -role cluster

		Logical	Status	Network	Current
Cur	rent Is	- 5			
		Interface	Admin/Oper	Address/Mask	Node
	t Hom				
					_
Clu	ster		,		
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1
01	e0a	true	,	160 054 0 5/00	
O 1	e0d	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1
UI	eua	true cluster1-02 clus1	up/up	169.254.3.8/23	cluster1
02	e0a	true	up/ up	109.254.5.0/25	Clustell
02	Coa	cluster1-02 clus2	up/up	169.254.3.9/23	cluster1-
02	e0d	true	∝r, ∝r	103,1201,013, 20	01000011
		cluster1-03 clus1	up/up	169.254.1.3/23	cluster1-
03	e0a	true			
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1
03	e0b	true			
		cluster1-04_clus1	up/up	169.254.1.6/23	cluster1
04	e0a	true			
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1
04	e0b	true			
8 e	ntries w	ere displayed.			

c. Verify that the cluster displays information for both cluster switches:

system cluster-switch show -is-monitoring-enabled-operational true

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch
                            Type
                                              Address
                           cluster-network 10.0.0.1
cs1
NX31320V
     Serial Number: FOXXXXXXGS
     Is Monitored: true
           Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(4)
   Version Source: CDP
                           cluster-network 10.0.0.2
cs2
NX3132QV
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
           Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(4)
   Version Source: CDP
2 entries were displayed.
```

3. Disable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif \* -auto
-revert false
```

4. On cluster switch cs2, shut down the ports connected to the cluster ports of the nodes.

```
cs2(config) # interface eth1/1/1-2,eth1/7-8
cs2(config-if-range) # shutdown
```

5. Verify that the cluster ports have migrated to the ports hosted on cluster switch cs1. This might take a few seconds.

```
network interface show -role cluster
```

		Logical	Status	Network	Current
Current	_				
Vserver		Interface	Admin/Oper	Address/Mask	Node
Port	_				
Cluster					
0145601		cluster1-01 clus1	up/up	169.254.3.4/23	cluster1-01
e0a	true	 e			
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0a	fals	se			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0a	true	е			
		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0a	fals	se			
		cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0a	true	е			
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0a	fals				
		cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0a	true				
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0a		se ere displayed.			

6. Verify that the cluster is healthy:

cluster show

cluster1::*> cluster		P14 -41 -41 -4	Dec 2 d l a m
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displ	ayed.		
<pre>cluster1::*></pre>			

- 7. Clean the configuration on switch cs2 and perform a basic setup.
 - a. Clean the configuration. This step requires a console connection to the switch.

```
cs2# write erase Warning: This command will erase the startup-configuration. Do you wish to proceed anyway? (y/n) [n] y cs2# reload This command will reboot the system. (y/n)? [n] y cs2#
```

- b. Perform a basic setup of the switch.
- 8. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference guides.

This example shows TFTP being used to copy an RCF to the bootflash on switch cs2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

9. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference guides.

This example shows the RCF file Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt being installed on switch cs2:

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-configecho-commands
```

10. Examine the banner output from the show banner motd command. You must read and follow the instructions under **Important Notes** to ensure the proper configuration and operation of the switch.

```
cs2# show banner motd
******************
*****
* NetApp Reference Configuration File (RCF)
* Switch : Cisco Nexus 3132Q-V
* Filename : Nexus 3132QV RCF v1.6-Cluster-HA-Breakout.txt
* Date : Nov-02-2020
* Version : v1.6
* Port Usage : Breakout configuration
* Ports 1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int e1/1/1-
* e1/2/1-4, e1/3/1-4, int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports 7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
* IMPORTANT NOTES
* - Load Nexus 3132QV RCF v1.6-Cluster-HA.txt for non breakout config
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
 cluster switch to be rebooted before the cluster becomes
operational.
* - Perform the following steps to ensure proper RCF installation:
   (1) Apply RCF, expect following messages:
       - Please save config and reload the system...
       - Edge port type (portfast) should only be enabled on ports...
       - TCAM region is not configured for feature QoS class IPv4...
   (2) Save running-configuration and reboot Cluster Switch
******************
*****
```

11. Verify that the RCF file is the correct newer version:

show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

- The RCF banner
- The node and port settings
- Customizations
 The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.
- 12. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference guides.

13. Reboot switch cs2. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs2# reload This command will reboot the system. (y/n)? [n] y
```

14. Apply the same RCF and save the running configuration for a second time.

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
cs2# copy running-config startup-config
[##################################] 100% Copy complete
```

- 15. Verify the health of cluster ports on the cluster.
 - a. Verify that e0d ports are up and healthy across all nodes in the cluster:

```
network port show -role cluster
```

```
Cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore

Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
```

		Q1			0000		h 1 + h
false	Cluster	Cluster		up	9000	auto/10000	neartny
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: clu	ster1-02						
Ignore							
Health						Speed (Mbps)	Health
	IPspace	Broadcast Do	omain	Link	MTU	Admin/Oper	Status
Status	1156000	210000000000000	711.01.2.11		1110	riamizii, opoz	
 e0a	 Cluster	Cluster		up	9000	auto/10000	healthy
Talse							
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: clu	ster1-03						
Ignore							
Health						Speed (Mbps)	Health
	IPspace	Broadcast Do	omain	Link	МТП	Admin/Oper	Status
Status							
	Cluster	Cluster		up	9000	auto/100000)
nealthy f	alse						
	Cluster	Cluster		up	9000	auto/100000)
nealthy f	alse						
Node: clu	ster1-04						
Ignore							
Uool+h						Speed (Mbps)	Health
Health Port	IPspace	Broadcast Do	omain	Link	МТП	Admin/Oper	Status
Status	110,000					Tiomizii, opoz	
e0a	Cluster	Cluster		up	9000	auto/100000)
healthy f							
e0d	Cluster	Cluster		up	9000	auto/100000)

b. Verify the switch health from the cluster (this might not show switch cs2, since LIFs are not homed on e0d).

Node/	Local	Discove	red		
Protocol	Port	Device	(LLDP: ChassisID)	Interface	
Platform					
					_
cluster1-0	1/cdp				
	e0a	cs1		Ethernet1/7	N3K-
C3132Q-V					
	e0d	cs2		Ethernet1/7	N3K-
C3132Q-V					
cluster01-	2/cdp				
	e0a	cs1		Ethernet1/8	N3K-
C3132Q-V					
	e0d	cs2		Ethernet1/8	N3K-
C3132Q-V					
cluster01-					
	e0a	cs1		Ethernet1/1/1	N3K-
C3132Q-V		_			_
~~1 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	e0b	cs2		Ethernet1/1/1	N3K-
C3132Q-V					
cluster1-0		4			
G21200 II	e0a	cs1		Ethernet1/1/2	N3K-
C3132Q-V	01	0		T.1 .1 /1 /0	3177
221200 FF	e0b	cs2		Ethernet1/1/2	N3K-
C3132Q-V					
al.,a+a.,1	*> ~::=+=	.m. al.ıa+a.	m arritah aharria	manitaning anable	J
-operation			L-SWICCH SHOW -IS-	-monitoring-enabled	ı
-operation Switch	ar true		Туре	Address	Model
				Audress	Mode:
cs1			cluster-network	10.233.205.90	N3K-
C3132Q-V					
	l Number	: FOXXXX	XXXGD		
Is M	onitored	l: true			
	Reason	: None			
	770	: Cisco N	Nexus Operating Sy	stem (NX-OS) Soft	ware,
Software	version	. 01000 1			
Software Version	version	. 01000 1			
	version	9.3(4)			

cs2 cluster-network 10.233.205.91 N3K-C3132Q-V
Serial Number: FOXXXXXXXGS
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
9.3(4)
Version Source: CDP
2 entries were displayed.

You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch:



2020 Nov 17 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK_CONSIST_PORT: Unblocking port port-channell on VLAN0092. Port consistency restored. 2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Blocking port-channell on VLAN0001. Inconsistent peer vlan. 2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Blocking port-channell on VLAN0092. Inconsistent local vlan.

16. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes.

The following example uses the interface example output from step 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

17. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds.

network interface show -role cluster

Cluster	1::">	> network interface			C
Current	Τα	Logical	Status	Network	Current
	_	Interface	Admin/Oper	Address/Mask	Node
Port			AdiiIII/Oper	Address/Mask	Node
	_				
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	fals	se			
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true	е			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	fals				
0.1		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0d	true	-	/	1.00 054 1 2/02	1 1 00
e0b	fals	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
eub	Idl		up/up	169.254.1.1/23	cluster1-03
e0b	true	-	up/up	109.254.1.1/25	Clustell-03
000	CIU	cluster1-04 clus1	מוו/מוו	169.254.1.6/23	cluster1-04
e0b	fals	-	αρ/αρ	103.201.1.0,20	01450011 01
		cluster1-04 clus2	up/up	169.254.1.7/23	cluster1-04
e0b	true	_			
8 entri	es we	ere displayed.			

18. Verify that the cluster is healthy:

cluster show

cluster1::*> cluster			
Node	Health	Eligibility 	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displ	ayed.		
cluster1::*>			

- 19. Repeat Steps 7 to 14 on switch cs1.
- 20. Enable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif \* -auto
-revert True
```

21. Reboot switch cs1. You do this to trigger the cluster LIFs to revert to their home ports. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs1# reload This command will reboot the system. (y/n)? [n] y
```

22. Verify that the switch ports connected to the cluster ports are up.

cs1# show	interface	brief	\ grep	up		
•	1	eth	access	up	none	10G(D)
 Eth1/1/2	1	eth	access	up	none	10G(D)
Eth1/7	1	eth	trunk	up	none	100G(D)
Eth1/8	1	eth	trunk	up	none	100G(D)
•						
•						

23. Verify that the ISL between cs1 and cs2 is functional:

show port-channel summary

24. Verify that the cluster LIFs have reverted to their home port:

network interface show -role cluster

cluster	1::*>	> network interface	show -role	cluster	
		Logical	Status	Network	Current
Current		T	7.1.1.70	7.11 /24 1	
Vserver		Interface	Admin/Oper	Address/Mask	Node
	_	=======================================			
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	true				
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true		,		
0.1		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	true	e cluster1-02 clus2	/n	169.254.3.9/23	cluster1-02
e0d	true	_	ир/ ир	109.234.3.9/23	Clustell-02
coa	CIU	cluster1-03 clus1	up/up	169.254.1.3/23	cluster1-03
e0b	true	_	-1, -1		
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	true	Э			
		cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	true				
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
	true				
		ere displayed.			
cluster	⊥::*>	>			

25. Verify that the cluster is healthy:

cluster show

cluster1::*> cluster			
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displ	ayed.		
cluster1::*>			

26. Ping the remote cluster interfaces to verify connectivity:

cluster ping-cluster -node local

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03 clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03 clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04 clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04 clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01 clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01 clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02 clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02 clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
. . . . . . . . . . . .
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
   Local 169.254.1.3 to Remote 169.254.1.7
   Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Migrate to a two-node switched cluster with Cisco Nexus 3132Q-V cluster switches

You must be aware of certain configuration information, port connections and cabling requirements when you migrate to a two-node switched cluster with Cisco Nexus 3132Q-V cluster switches.

- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco ® Cluster Network Switch Reference Configuration File Download page.
- The cluster switches use the Inter-Switch Link (ISL) ports e1/31-32.
- The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
 - The nodes with 10 GbE cluster connections require QSFP optical modules with breakout fiber cables or QSFP to SFP+ copper break-out cables.
 - The nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28 optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
 - The cluster switches use the appropriate ISL cabling: 2x QSFP28 fiber or copper direct-attach cables.
- On Nexus 3132Q-V, you can operate QSFP ports as either 40/100 Gb Ethernet or 4 x10 Gb Ethernet modes.

By default, there are 32 ports in the 40/100 Gb Ethernet mode. These 40 Gb Ethernet ports are numbered in a 2-tuple naming convention. For example, the second 40 Gb Ethernet port is numbered as 1/2. The process of changing the configuration from 40 Gb Ethernet to 10 Gb Ethernet is called *breakout* and the process of changing the configuration from 10 Gb Ethernet to 40 Gb Ethernet is called *breakin*. When you break out a 40/100 Gb Ethernet port into 10 Gb Ethernet ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40/100 Gb Ethernet port are numbered as 1/2/1, 1/2/2, 1/2/3, 1/2/4.

• On the left side of Nexus 3132Q-V is a set of four SFP+ ports multiplexed to the first QSFP port.

By default, the RCF is structured to use the first QSFP port.

You can make four SFP+ ports active instead of a QSFP port for Nexus 3132Q-V by using the hardware profile front portmode sfp-plus command. Similarly, you can reset Nexus 3132Q-V to use a QSFP port instead of four SFP+ ports by using the hardware profile front portmode qsfp command.

• You must have configured some of the ports on Nexus 3132Q-V to run at 10 GbE or 40/100 GbE.

You can break-out the first six ports into 4x10 GbE mode by using the interface breakout module 1 port 1-6 map 10g-4x command. Similarly, you can regroup the first six QSFP+ ports from breakout configuration by using the no interface breakout module 1 port 1-6 map 10g-4x command.

• You must have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.

The Cisco Ethernet Switches page has information about the ONTAP and NX-OS versions supported in this procedure.

How to migrate a two-node switched cluster with Cisco Nexus 3132Q-V cluster switches

If you have a two-node switchless cluster, you can migrate nondisruptively to a two-node switched cluster that includes Cisco Nexus 3132Q-V cluster network switches.

Before you begin

- The configurations must be properly set up and functioning.
- The nodes must be running ONTAP 9.4 or later.

- All cluster ports must be in the up state.
- The Cisco Nexus 3132Q-V cluster switch must be supported.
- The existing cluster network configuration must have:
 - The Nexus 3132 cluster infrastructure that is redundant and fully functional on both switches.

The latest RCF and NX-OS versions on your switches.

- Management connectivity on both switches.
- · Console access to both switches.
- All cluster logical interfaces (LIFs) in the up state without being migrated.
- Initial customization of the switch.
- All the ISL ports enabled and cabled.

About this task

The examples in this procedure use the following switch and node nomenclature:

- Nexus 3132Q-V cluster switches, C1 and C2.
- The nodes are n1 and n2.



The examples in this procedure use two nodes, each utilizing two 40/100 GbE cluster interconnect ports e4a and e4e. The Hardware Universe has details about the cluster ports on your platforms.

- n1 clus1 is the first cluster logical interface (LIF) to be connected to cluster switch C1 for node n1.
- n1_clus2 is the first cluster LIF to be connected to cluster switch C2 for node n1.
- n2 clus1 is the first cluster LIF to be connected to cluster switch C1 for node n2.
- n2 clus2 is the second cluster LIF to be connected to cluster switch C2 for node n2.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco ® Cluster Network Switch Reference Configuration File Download page.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

- The cluster starts with two nodes connected and functioning in a two-node switchless cluster setting.
- The first cluster port moved to C1 (Steps 1- 20)
- The second cluster port moved to C2 (Steps 21- 32).
- Disable the two-node switchless cluster option (Steps 33- 35)

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

- 2. Determine the administrative or operational status for each cluster interface:
 - a. Display the network port attributes:

network port show

```
cluster::*> network port show -role cluster
 (network port show)
Node: n1
Ignore
                                  Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
______
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
Node: n2
Ignore
                                  Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
______ ______
----
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
4 entries were displayed.
```

b. Display information about the logical interfaces:

network interface show

cluster	::*>	network in	terface show	w -role cluster					
(netwo	(network interface show)								
		Logical	Status	Network	Current				
Current	Is								
Vserver		Interface	Admin/Oper	Address/Mask	Node				
Port	Hom	е							
		_							
Cluster									
		n1_clus1	up/up	10.10.0.1/24	n1				
e4a	tru	е							
		n1_clus2	up/up	10.10.0.2/24	n1				
e4e	tru	е							
		n2_clus1	up/up	10.10.0.3/24	n2				
e4a	tru	е							
		n2_clus2	up/up	10.10.0.4/24	n2				
e4e	tru	е							
4 entri	4 entries were displayed.								

 Verify that the appropriate RCFs and image are installed on the new 3132Q-V switches as necessary for your requirements, and make any essential site customizations, such as users and passwords, network addresses, and so on.

You must prepare both switches at this time. If you need to upgrade the RCF and image software, you must follow these steps:

- a. Go to the Cisco Ethernet Switches page on the NetApp Support Site.
- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software.
- 4. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- 5. On Nexus 3132Q-V switches C1 and C2, disable all node-facing ports C1 and C2, but do not disable the ISL ports.

The following example shows ports 1 through 30 being disabled on Nexus 3132Q-V cluster switches C1 and C2 using a configuration supported in RCF

```
C1# copy running-config startup-config
[############ 100%
Copy complete.
C1# configure
C1 (config) # int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range) # shutdown
C1(config-if-range) # exit
C1(config)# exit
C2# copy running-config startup-config
[############ 100%
Copy complete.
C2# configure
C2 (config) # int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4.e1/7-30
C2(config-if-range) # shutdown
C2(config-if-range) # exit
C2(config)# exit
```

- 6. Connect ports 1/31 and 1/32 on C1 to the same ports on C2 using supported cabling.
- 7. Verify that the ISL ports are operational on C1 and C2:

```
show port-channel summary
```

```
C1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
      I - Individual  H - Hot-standby (LACP only)
      s - Suspended r - Module-removed
      S - Switched R - Routed
      U - Up (port-channel)
     M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/31(P) Eth1/32(P)
C2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
      I - Individual  H - Hot-standby (LACP only)
      s - Suspended r - Module-removed
      S - Switched R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
_____
Group Port- Type Protocol Member Ports
    Channel
1 Po1(SU) Eth LACP Eth1/31(P) Eth1/32(P)
```

8. Display the list of neighboring devices on the switch:

show cdp neighbors

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                 Local Intrfce Hldtme Capability Platform
                                                                Port
ID
C2
                 Eth1/31
                               174 RSIS
                                                  N3K-C3132Q-V
Eth1/31
C2
                  Eth1/32
                                174 RSIS
                                                  N3K-C3132Q-V
Eth1/32
Total entries displayed: 2
C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                 Local Intrfce Hldtme Capability Platform
                                                                Port
ID
C1
                 Eth1/31
                               178
                                      RSIs
                                                  N3K-C3132Q-V
Eth1/31
C1
                  Eth1/32
                                178 RSIS
                                                  N3K-C3132Q-V
Eth1/32
Total entries displayed: 2
```

9. Display the cluster port connectivity on each node:

network device-discovery show

The following example shows a two-node switchless cluster configuration.

cluster::*> network device-discovery show							
	Local	Discovered					
Node	Port	Device	Interface	Platform			
n1	/cdp						
	e4a	n2	e4a	FAS9000			
	e4e	n2	e4e	FAS9000			
n2	/cdp						
	e4a	n1	e4a	FAS9000			
	e4e	n1	e4e	FAS9000			

10. Migrate the clus1 interface to the physical port hosting clus2:

network interface migrate

Execute this command from each local node.

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1
-destination-node n1 -destination-port e4e
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2
-destination-node n2 -destination-port e4e
```

11. Verify the cluster interfaces migration:

network interface show

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>								
	Logical	Status	Network	Current				
Current Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
	_							
Cluster								
	n1_clus1	up/up	10.10.0.1/24	n1	e4e			
false								
	n1_clus2	up/up	10.10.0.2/24	n1	e4e			
true		,						
	n2_clus1	up/up	10.10.0.3/24	n2	e4e			
false	0 1 0	,	10 10 0 1/01	0	4			
	nz_clus2	up/up	10.10.0.4/24	n2	e4e			
true 4 entries we	ere display	ed.						

12. Shut down cluster ports clus1 LIF on both nodes:

network port modify

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

13. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus2 n1
                     e4e 10.10.0.2
Cluster n2 clus2 n2
                     e4e 10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 32 path(s):
   Local 10.10.0.1 to Remote 10.10.0.3
   Local 10.10.0.1 to Remote 10.10.0.4
   Local 10.10.0.2 to Remote 10.10.0.3
   Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

14. Disconnect the cable from e4a on node n1.

You can refer to the running configuration and connect the first 40 GbE port on the switch C1 (port 1/7 in this example) to e4a on n1 using supported cabling on Nexus 3132Q-V.



When reconnecting any cables to a new Cisco cluster switch, the cables used must be either fiber or cabling supported by Cisco.

15. Disconnect the cable from e4a on node n2.

You can refer to the running configuration and connect e4a to the next available 40 GbE port on C1, port 1/8, using supported cabling.

16. Enable all node-facing ports on C1.

The following example shows ports 1 through 30 being enabled on Nexus 3132Q-V cluster switches C1 and C2 using the configuration supported in RCF

```
NX3132 RCF v1.1 24p10g 26p40g.txt:
```

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

17. Enable the first cluster port, e4a, on each node:

network port modify

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

18. Verify that the clusters are up on both nodes:

network port show

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
Node: n2
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 - e4e Cluster up 9000 auto/40000 -
e4e
4 entries were displayed.
```

19. For each node, revert all of the migrated cluster interconnect LIFs:

```
network interface revert
```

The following example shows the migrated LIFs being reverted to their home ports.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

20. Verify that all of the cluster interconnect ports are now reverted to their home ports:

```
network interface show
```

The Is Home column should display a value of true for all of the ports listed in the Current Port column. If the displayed value is false, the port has not been reverted.

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>								
(Status	Network	Current				
Current Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
	_							
Cluster								
	n1_clus1	up/up	10.10.0.1/24	n1	e4a			
true	1 7 0	,	10 10 0 0 /04	4				
.	nl_clus2	up/up	10.10.0.2/24	n1	e4e			
true	n2 alua1	/	10.10.0.3/24	~ ?	e4a			
true	IIZ_CIUSI	սք/ սք	10.10.0.3/24	112	e4a			
crue	n2 clus2	un/un	10.10.0.4/24	n 2	e4e			
true		αρ/αρ	10.10.0.1/21	114	0.10			
4 entries we	ere display	ed.						

21. Display the cluster port connectivity on each node:

network device-discovery show

cluster::	*> networ	rk device-discovery Discovered	show	
Node	Port	Device	Interface	Platform
n1	 /cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	n1	e4e	FAS9000

22. On the console of each node, migrate clus2 to port e4a:

network interface migrate

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2
-destination-node n2 -destination-port e4a
```

23. Shut down cluster ports clus2 LIF on both nodes:

```
network port modify
```

The following example shows the specified ports being shut down on both nodes:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

24. Verify the cluster LIF status:

network interface show

cluster::*>	network in	terface show	w -role cluster					
(network interface show)								
	Logical	Status	Network	Current				
Current Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
	_							
Cluster								
	n1_clus1	up/up	10.10.0.1/24	n1	e4a			
true								
6 3	n1_clus2	up/up	10.10.0.2/24	n1	e4a			
false	0 1 1	,	10 10 0 0 /04		4			
	n2_clus1	up/up	10.10.0.3/24	n2	e4a			
true	n) alua?	/	10 10 0 4/24	n2	0/10			
false	IIZ_CTUSZ	up/up	10.10.0.4/24	112	e4a			
4 entries w	ere dienlass	ad						
4 elicites w	ere dispiay	- u.						

25. Disconnect the cable from e4e on node n1.

You can refer to the running configuration and connect the first 40 GbE port on the switch C2 (port 1/7 in this example) to e4e on n1 using supported cabling on Nexus 3132Q-V.

26. Disconnect the cable from e4e on node n2.

You can refer to the running configuration and connect e4e to the next available 40 GbE port on C2, port 1/8, using supported cabling.

27. Enable all node-facing ports on C2.

The following example shows ports 1 through 30 being enabled on Nexus 3132Q-V cluster switches C1 and C2 using a configuration supported in RCF

```
NX3132 RCF v1.1 24p10g 26p40g.txt:
```

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

28. Enable the second cluster port, e4e, on each node:

```
network port modify
```

The following example shows the specified ports being brought up:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> network port modify -node n2 -port e4e -up-admin true
```

29. For each node, revert all of the migrated cluster interconnect LIFs:

```
network interface revert
```

The following example shows the migrated LIFs being reverted to their home ports.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

30. Verify that all of the cluster interconnect ports are now reverted to their home ports:

```
network interface show
```

The Is Home column should display a value of true for all of the ports listed in the Current Port column. If the displayed value is false, the port has not been reverted.

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>								
G	Logical	Status	Network	Current				
Current Is		- 1 / / 0	/					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
	-							
Cluster								
	n1 clus1	up/up	10.10.0.1/24	n1	e4a			
true	_							
	n1 clus2	up/up	10.10.0.2/24	n1	e4e			
true	_	1						
	n2 clus1	מוו/מוו	10.10.0.3/24	n2	e4a			
true		ω _P , ω _P	10.10.00, 21		010			
CIUC	n? clus?	110/110	10.10.0.4/24	n2	e4e			
true	112_01432	αρ/ αρ	10.10.0.1/21	114	OFC			
	vere display							

^{31.} Verify that all of the cluster interconnect ports are in the ${\tt up}$ state.

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
Node: n2
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 - e4e Cluster up 9000 auto/40000 -
4 entries were displayed.
```

32. Display the cluster switch port numbers each cluster port is connected to on each node:

network device-discovery show

clus	ster::*> ne Local	twork device-dis Discovered	covery show	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

33. Display discovered and monitored cluster switches:

system cluster-switch show

cluster::*> system cluster-switch show Type Address Model C1 cluster-network 10.10.1.101 NX3132V Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP C2 cluster-network 10.10.1.102 NX3132V Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP 2 entries were displayed.

34. Disable the two-node switchless configuration settings on any node:

network options switchless-cluster

network options switchless-cluster modify -enabled false

35. Verify that the switchless-cluster option has been disabled.

 ${\tt network\ options\ switchless-cluster\ show}$

36. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e4a 10.10.0.1
Cluster n1 clus2 n1
                     e4e 10.10.0.2
Cluster n2_clus1 n2 e4a 10.10.0.3
Cluster n2 clus2 n2
                     e4e 10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 1500 byte MTU on 32 path(s):
   Local 10.10.0.1 to Remote 10.10.0.3
   Local 10.10.0.1 to Remote 10.10.0.4
   Local 10.10.0.2 to Remote 10.10.0.3
   Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

37. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

```
system cluster-switch log setup-password
system cluster-switch log enable-collection
```

```
cluster::*> **system cluster-switch log setup-password**
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

38. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Replace Cisco Nexus 3132Q-V cluster switches

You must be aware of certain configuration information, port connections and cabling requirements when you replace Cisco Nexus 3132Q-V cluster switches.

- The Cisco Nexus 3132Q-V cluster switch is supported.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.
- The cluster switches use the Inter-Switch Link (ISL) ports e1/31-32.
- The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
 - The nodes with 10 GbE cluster connections require QSFP optical modules with breakout fiber cables or QSFP to SFP+ copper break-out cables.
 - The nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28 optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
 - The cluster switches use the appropriate ISL cabling: 2x QSFP28 fiber or copper direct-attach cables.
- On Nexus 3132Q-V, you can operate QSFP ports as either 40/100 Gb Ethernet or 4 x10 Gb Ethernet modes.

By default, there are 32 ports in the 40/100 Gb Ethernet mode. These 40 Gb Ethernet ports are numbered in a 2-tuple naming convention. For example, the second 40 Gb Ethernet port is numbered as 1/2. The process of changing the configuration from 40 Gb Ethernet to 10 Gb Ethernet is called *breakout* and the process of changing the configuration from 10 Gb Ethernet to 40 Gb Ethernet is called *breakin*. When you break out a 40/100 Gb Ethernet port into 10 Gb Ethernet ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40/100 Gb Ethernet port are numbered as 1/2/1, 1/2/2, 1/2/3, 1/2/4.

• On the left side of Nexus 3132Q-V is a set of four SFP+ ports multiplexed to the first QSFP port.

By default, the RCF is structured to use the first QSFP port.

You can make four SFP+ ports active instead of a QSFP port for Nexus 3132Q-V by using the hardware profile front portmode sfp-plus command. Similarly, you can reset Nexus 3132Q-V to use a QSFP port instead of four SFP+ ports by using the hardware profile front portmode qsfp command.

• You must have configured some of the ports on Nexus 3132Q-V to run at 10 GbE or 40/100 GbE.

You can break-out the first six ports into 4x10 GbE mode by using the interface breakout module 1 port 1-6 map 10g-4x command. Similarly, you can regroup the first six QSFP+ ports from breakout configuration by using the no interface breakout module 1 port 1-6 map 10g-4x command.

• You must have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.

The Cisco Ethernet Switches page has information about the ONTAP and NX-OS versions supported in this procedure.

How to replace Cisco Nexus 3132Q-V cluster switches

Replacing a defective Cisco Nexus 3132Q-V switch in a cluster network is a nondisruptive procedure (NDO), and you must perform a specific sequence of tasks.

Before you begin

• The existing cluster and network configuration must have:

The Nexus 3132Q-V cluster infrastructure must be redundant and fully functional on both switches.

The Cisco Ethernet Switch page has the latest RCF and NX-OS versions on your switches.

- ° All cluster ports must be in the up state.
- Management connectivity must exist on both switches.
- All cluster logical interfaces (LIFs) must be in the up state and must not have been migrated.
- The Nexus 3132Q-V replacement switch:
 - Management network connectivity on the replacement switch must be functional.
 - Console access to the replacement switch must be in place.
 - The desired RCF and NX-OS operating system image switch must be loaded onto the switch.
 - · Initial customization of the switch must be complete.

About this task

This procedure replaces the second Nexus 3132Q-V cluster switch CL2 with new 3132Q-V switch C2. The examples in this procedure use the following switch and node nomenclature:

- n1 clus1 is the first cluster logical interface (LIF) connected to cluster switch C1 for node n1.
- n1 clus2 is the first cluster LIF connected to cluster switch CL2 or C2, for node n1.
- n1 clus3 is the second LIF connected to cluster switch C2, for node n1.
- n1 clus4 is the second LIF connected to cluster switch CL1, for node n1.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.
- The nodes are n1, n2, n3, and n4.

The examples in this procedure use four nodes: Two nodes use four 10 GB cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40 GB cluster interconnect ports: e4a and e4e. See the Hardware Universe for the actual cluster ports on your platforms.

This procedure covers the following scenario:

- The cluster starts with four nodes connected to two Nexus 3132Q-V cluster switches, CL1 and CL2.
- Cluster switch CL2 is to be replaced by C2 (Steps 1 -21)
 - On each node, cluster LIFs connected to CL2 are migrated onto cluster ports connected to CL1.
 - Disconnect cabling from all ports on CL2 and reconnect cabling to the same ports on the replacement switch C2.
 - On each node, its migrated cluster LIFs are reverted.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Display information about the devices in your configuration:

network device-discovery show

		Discovered	T. 1. C	D1 + C
		Device	Interface	Platform
11	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	CL2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	CL1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	CL2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	CL1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3132Q-V
	e4e	CL2	Ethernet1/7	N3K-C3132Q-V
n 4	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3132Q-V
	e4e	CL2	Ethernet1/8	N3K-C3132Q-V

- 3. Determine the administrative or operational status for each cluster interface:
 - a. Display the network port attributes:

network port show

Status							
e0a -	Cluster	Cluster		up	9000	auto/10000	-
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d -	Cluster	Cluster		up	9000	auto/10000	-
Node: n2							
Ignore							
Health						Speed(Mbps)	Health
Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a -	Cluster	Cluster		up	9000	auto/10000	-
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c -	Cluster	Cluster		up	9000	auto/10000	-
e0d -	Cluster	Cluster		up	9000	auto/10000	-
Node: n3							
Ignore							
Health						Speed(Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e4a -	Cluster	Cluster		up	9000	auto/40000	-
e4e -	Cluster	Cluster		up	9000	auto/40000	-
Node: n4							

Ignore				Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast Domai	in Link MTU	-	Status
e4a	Cluster	Cluster	up 900	00 auto/40000	_
e4e -	Cluster	Cluster	up 900	00 auto/40000	_

b. Display information about the logical interfaces:

12 entries were displayed.

network interface show

		Logical	Status	Network	Current
Current					
			Admin/Oper	Address/Mask	Node
Port	HOM:	e 			
		_			
Cluster					
		n1_clus1	up/up	10.10.0.1/24	n1
e0a	tru				
0.1		_	up/up	10.10.0.2/24	n1
e0b	tru		110/110	10.10.0.3/24	n1
e0c	tru	-	up/ up	10.10.0.3/24	111
	cra		up/up	10.10.0.4/24	n1
e0d	tru	_	1 1		
		n2_clus1	up/up	10.10.0.5/24	n2
e0a	tru				
01		_	up/up	10.10.0.6/24	n2
e0b	tru		11n / 11n	10.10.0.7/24	n2
e0c	tru	_	ир/ ир	10.10.0.7/24	112
			up/up	10.10.0.8/24	n2
e0d	tru	_			
		n3_clus1	up/up	10.10.0.9/24	n3
e0a	tru		,		_
0		_	up/up	10.10.0.10/24	n3
e0e	tru		up/up	10.10.0.11/24	n4
e0a	tru	_	up/ up	10.10.0.11/24	114
-		n4_clus2	up/up	10.10.0.12/24	n4
e0e	tru	_			

c. Display the information on the discovered cluster switches:

system cluster-switch show

```
cluster::> system cluster-switch show
Switch
                            Type
                                               Address
                                                                Model
_____
                            cluster-network 10.10.1.101
CT<sub>1</sub>1
NX3132V
     Serial Number: FOX000001
     Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3) I4(1)
    Version Source: CDP
CL2
                             cluster-network 10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3) I4(1)
    Version Source: CDP
2 entries were displayed.
```

4. Verify that the appropriate RCF and image are installed on the new Nexus 3132Q-V switch as necessary for your requirements, and make any essential site customizations.

You must prepare the replacement switch at this time. If you need to upgrade the RCF and image, you must follow these steps:

- a. On the NetApp Support Site, go to the Cisco Ethernet Switch page.
- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of the RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software.
- 5. Migrate the LIFs associated to the cluster ports connected to switch C2:

```
network interface migrate
```

This example shows that the LIF migration is done on all the nodes:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2 -source-node n1 -destination-node n1 -destination-port e0a cluster::*> network interface migrate -vserver Cluster -lif n1_clus3 -source-node n1 -destination-node n1 -destination-port e0d cluster::*> network interface migrate -vserver Cluster -lif n2_clus2 -source-node n2 -destination-node n2 -destination-port e0a cluster::*> network interface migrate -vserver Cluster -lif n2_clus3 -source-node n2 -destination-node n2 -destination-port e0d cluster::*> network interface migrate -vserver Cluster -lif n3_clus2 -source-node n3 -destination-node n3 -destination-port e4a cluster::*> network interface migrate -vserver Cluster -lif n4_clus2 -source-node n4 -destination-node n4 -destination-port e4a
```

6. Verify cluster's health:

network interface show

<pre>cluster::*> network interface show -role cluster</pre>							
	Logical	Status	Network	Current			
Current Is Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port		
Cluster							
true	n1_clus1	up/up	10.10.0.1/24	n1	e0a		
01 40	n1_clus2	up/up	10.10.0.2/24	n1	e0a		
false	n1_clus3	up/up	10.10.0.3/24	n1	e0d		
false	n1_clus4	up/up	10.10.0.4/24	n1	e0d		
true	n2_clus1	up/up	10.10.0.5/24	n2	e0a		
true	n2_clus2	up/up	10.10.0.6/24	n2	e0a		
false	n2_clus3	up/up	10.10.0.7/24	n2	e0d		
false	n2 clus4	up/up	10.10.0.8/24	n2	e0d		
true	n3 clus1	up/up	10.10.0.9/24	n3	e4a		
true	n3_clus2	up/up	10.10.0.10/24	n3	e4a		
false		up/up	10.10.0.11/24	n4	e4a		
true	_						
false	_	up/up yed.	10.10.0.12/24	n4	e4a		

7. Shut down the cluster interconnect ports that are physically connected to switch CL2:

network port modify

This example shows the specified ports being shut down on all nodes:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false cluster::*> network port modify -node n1 -port e0c -up-admin false cluster::*> network port modify -node n2 -port e0b -up-admin false cluster::*> network port modify -node n2 -port e0c -up-admin false cluster::*> network port modify -node n3 -port e4e -up-admin false cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1
                      e0a 10.10.0.1
Cluster n1 clus2 n1
                      e0b 10.10.0.2
Cluster n1 clus3 n1
                      e0c 10.10.0.3
                     e0d 10.10.0.4
Cluster n1 clus4 n1
                      e0a 10.10.0.5
Cluster n2 clus1 n2
Cluster n2 clus2 n2
                      e0b 10.10.0.6
Cluster n2 clus3 n2
                      e0c 10.10.0.7
Cluster n2 clus4 n2
                      e0d 10.10.0.8
Cluster n3 clus1 n4
                      e0a 10.10.0.9
Cluster n3 clus2 n3
                      e0e 10.10.0.10
                      e0a 10.10.0.11
Cluster n4 clus1 n4
Cluster n4 clus2 n4
                      e0e 10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
```

```
Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

9. Shut down the ports 1/31 and 1/32 on CL1, and the active Nexus 3132Q-V switch:

shutdown

This example shows the ISL ports 1/31 and 1/32 being shut down on switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1(config-if-range) # shutdown
(CL1(config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

10. Remove all the cables attached to the Nexus 3132Q-V switch CL2 and reconnect them to the replacement switch C2 on all nodes.

- 11. Remove the ISL cables from ports e1/31 and e1/32 on CL2 and reconnect them to the same ports on the replacement switch C2.
- 12. Bring up ISLs ports 1/31 and 1/32 on the Nexus 3132Q-V switch CL1.

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1 (config-if-range) # no shutdown
(CL1 (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

13. Verify that the ISLs are up on CL1:

```
show port-channel
```

Ports Eth1/31 and Eth1/32 should indicate (P), which means that the ISL ports are up in the port-channel.

14. Verify that the ISLs are up on C2:

```
show port-channel summary
```

Ports Eth1/31 and Eth1/32 should indicate (P), which means that both ISL ports are up in the portchannel.

15. On all nodes, bring up all the cluster interconnect ports connected to the Nexus 3132Q-V switch C2: network port modify

```
cluster::*> network port modify -node n1 -port e0b -up-admin true cluster::*> network port modify -node n1 -port e0c -up-admin true cluster::*> network port modify -node n2 -port e0b -up-admin true cluster::*> network port modify -node n2 -port e0c -up-admin true cluster::*> network port modify -node n3 -port e4e -up-admin true cluster::*> network port modify -node n4 -port e4e -up-admin true
```

16. For all nodes, revert all of the migrated cluster interconnect LIFs:

network interface revert

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
Cluster::*> network interface revert -vserver Cluster -lif n3_clus2
Cluster::*> network interface revert -vserver Cluster -lif n4_clus2
```

17. Verify that the cluster interconnect ports are now reverted to their home:

```
network interface show
```

This example shows that all the LIFs are successfully reverted because the ports listed under the Current Port column have a status of true in the Is Home column. If the Is Home column value is false, the LIF has not been reverted.

	Logical	Status	Network	Current	
Current Is Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster		/	10 10 0 1/24	n1	e0a
true	n1_clus1	up/up	10.10.0.1/24	111	eua
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true	n1 alua/	/n	10.10.0.4/24	n1	e0d
true	n1_clus4	up/up	10.10.0.4/24	111	eua
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true	n2 clus3	up/up	10.10.0.7/24	n2	e0c
true	II2_Cluss	ир/ ир	10.10.0.7/24	112	e00
true	n2_clus4	up/up	10.10.0.8/24	n2	e0d
crue	n3_clus1	up/up	10.10.0.9/24	n3	e4a
true	n3 clus2	up/up	10.10.0.10/24	n3	e4e
true	113_01402	αρ, αρ	10.10.0.10,21	110	010
true	n4_clus1	up/up	10.10.0.11/24	n4	e4a
0140	n4 clus2	up/up	10.10.0.12/24	n4	e4e

18. Verify that the cluster ports are connected:

network port show

Health Port	IPspace	Proadcast	Domain	Tink	MTI	Admin/Oper	C+o+us	
Status	irspace	bloadcast	DOMATH	ПТПК	MIO	Admitit/Oper	Status	
e0a	Cluster	Cluster		up	9000	auto/10000	-	-
e0b	Cluster	Cluster		up	9000	auto/10000	-	-
e0c	Cluster	Cluster		up	9000	auto/10000	-	-
e0d	Cluster	Cluster		up	9000	auto/10000	-	-
Node: n2								
Ignore						Spood (Mbpg)	Hoolth	
Health						Speed (Mbps)	пеатип	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
Status								
e0a	Cluster	Cluster		up	9000	auto/10000	_	_
e0a e0b	Cluster	Cluster		up	9000			_
e0b e0c	Cluster	Cluster		up	9000			_
e0d	Cluster	Cluster		_	9000			_
eud	Cluster	Cluster		up	9000	aut0/10000	_	_
Node: n3								
Ignore								
						Speed(Mbps)	Health	
Health								
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
Status								
	Cl., c. t. c	C1			0000			
e4a e4e	Cluster Cluster			_		auto/40000 auto/40000		
e4e	Cluster	Cluster		up	9000	aut0/40000	_	_
Node: n4								
Ignore						Spood (Mhns)	Uool+h	
Health						Speed (Mbps)	11Eal Ull	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
Status							, , , , , , , , , , , , , , , , , , , ,	
e4a	Cluster	Cluster		up	9000	auto/40000	-	-

```
e4e Cluster Cluster up 9000 auto/40000 - - 12 entries were displayed.
```

19. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1
                      e0a 10.10.0.1
Cluster n1 clus2 n1
                      e0b 10.10.0.2
                      e0c 10.10.0.3
e0d 10.10.0.4
Cluster n1 clus3 n1
Cluster n1 clus4 n1
Cluster n2 clus1 n2
                      e0a 10.10.0.5
Cluster n2 clus2 n2 e0b 10.10.0.6
Cluster n2 clus3 n2
                      e0c 10.10.0.7
Cluster n2 clus4 n2 e0d 10.10.0.8
Cluster n3 clus1 n3
                      e0a 10.10.0.9
Cluster n3 clus2 n3
                      e0e 10.10.0.10
Cluster n4 clus1 n4
                      e0a 10.10.0.11
Cluster n4 clus2 n4
                        e0e 10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
```

```
Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

20. Display the information about the devices in your configuration:

```
° network device-discovery show
```

[°] network port show -role cluster

[°] network interface show -role cluster

[°] system cluster-switch show

Clustel:./		device-discovery Discovered	SHOW	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V
12 entries	were dis	splayed.		

	*> network po k port show)	rt show -rol	e clus	ster			
Ignore						Speed(Mbps)	Health
Health						speed (Mpps)	nearth
Port	IPspace	Broadcast D	omain	Link	MTU	Admin/Oper	Status
Status							
e0a	 Cluster	Cluster		1110	9000	auto/10000	_
	CIUSCEI	Clustel		uр	3000	aut0/10000	
e0b	Cluster	Cluster		up	9000	auto/10000	_
_							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-	Cluston	Cluston		1170	0000	211+2/10000	
e0d -	Cluster	cruster		uр	9000	auto/10000	_
Node: n2							

Ignore						G 1/25	7.1
Health						Speed(Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a	 Cluster	Cluster		up	9000	auto/10000	_
-				-			
e0b	Cluster	Cluster		up	9000	auto/10000	-
- e0c	Cluster	Cluster		up	9000	auto/10000	_
-				1		·	
e0d	Cluster	Cluster		up	9000	auto/10000	-
_							
Node: n3							
Ignore						Speed(Mbps)	Health
Health						opeca (nopo)	11001011
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e4a	Cluster	Cluster		up	9000	auto/40000	-
-	Cluster	Clustor		110	0000	auto/40000	_
-	Cluster	Cluster		up	9000	aut0/40000	_
Node: n4							
Ignore							
_						Speed (Mbps)	Health
Health	T.D	D	Dec '	т д 1	NACTION	7 alm 1 - / 0	0++
Port Status	IPspace	Broadcast	Domain	Link	M.I.N	Admin/Oper	Status
e4a -	Cluster	Cluster		up	9000	auto/40000	_
e4e	Cluster	Cluster		up	9000	auto/40000	-
				-			

12 entries were displayed.

		Status	Network	Current
	Interface	Admin/Oper	Address/Mask	Node
Port 	ноте 			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true	,		
- 01-	-	up/up	10.10.0.2/24	n1
e0b	true	11n/11n	10.10.0.3/24	n1
e0c	true	ир/ ир	10.10.0.3/24	111
		up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
0.1	-	up/up	10.10.0.6/24	n2
e0b	true	up/up	10.10.0.7/24	n2
e0c	true	ир/ ир	10.10.0.7/24	112
	n2 clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true	,		
0.10	_	up/up	10.10.0.10/24	n3
e4e	true n4 clus1	מוו/מוו	10.10.0.11/24	n4
e4a	true	ар/ ар	10.10.0.11/24	11.1
	n4 clus2	up/up	10.10.0.12/24	n4
	_			

cluster::*> system cluster-switch show

Switch Type Address Model

CL1 cluster-network 10.10.1.101 NX3132V

Serial Number: FOX000001

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software,

Version

7.0(3) I4(1)

Version Source: CDP

CL2 cluster-network 10.10.1.102 NX3132V

Serial Number: FOX000002

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software,

Version

7.0(3) I4(1)

Version Source: CDP

C2 cluster-network 10.10.1.103 NX3132V

Serial Number: FOX000003

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software,

Version

7.0(3)14(1)

Version Source: CDP

3 entries were displayed.

21. Remove the replaced Nexus 3132Q-V switch, if it is not already removed automatically:

system cluster-switch delete

cluster::*> system cluster-switch delete -device CL2

22. Verify that the proper cluster switches are monitored:

system cluster-switch show

cluster::> system cluster-switch show Type Address cluster-network 10.10.1.101 NX3132V CL1 Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP C2 cluster-network 10.10.1.103 NX3132V Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP 2 entries were displayed.

23. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

system cluster-switch log setup-password
system cluster-switch log enable-collection

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

24. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

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

Related information

Cisco Ethernet Switch description page

Hardware Universe

Replace a Cisco Nexus 5596 cluster switch with a Cisco Nexus 3132Q-V cluster switch

You must be aware of certain configuration information, port connections and cabling requirements when you are replacing a Cisco Nexus 5596 cluster switch with a Cisco Nexus 3132Q-V cluster switch.

- The following cluster switches are supported:
 - Nexus 5596
 - Nexus 3132Q-V
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.
- The cluster switches use the following ports for connections to nodes:
 - Ports e1/1-40 (10 GbE): Nexus 5596
 - Ports e1/1-30 (40/100 GbE): Nexus 3132Q-V
- The cluster switches use the following Inter-Switch Link (ISL) ports:
 - Ports e1/41-48 (10 GbE): Nexus 5596
 - Ports e1/31-32 (40/100 GbE): Nexus 3132Q-V
- The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
 - Nodes with 10 GbE cluster connections require QSFP to SFP+ optical fiber breakout cables or QSFP to SFP+ copper breakout cables.
 - Nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
- The cluster switches use the appropriate ISL cabling:
 - Beginning: Nexus 5596 to Nexus 5596 (SFP+ to SFP+)
 - 8x SFP+ fiber or copper direct-attach cables
 - Interim: Nexus 5596 to Nexus 3132Q-V (QSFP to 4xSFP+ break-out)
 - 1x QSFP to SFP+ fiber break-out or copper break-out cables
 - Final: Nexus 3132Q-V to Nexus 3132Q-V (QSFP28 to QSFP28)
 - 2x QSFP28 fiber or copper direct-attach cables
- On Nexus 3132Q-V switches, you can operate QSFP/QSFP28 ports as either 40/100 Gigabit Ethernet or 4 x10 Gigabit Ethernet modes.

By default, there are 32 ports in the 40/100 Gigabit Ethernet mode. These 40 Gigabit Ethernet ports are numbered in a 2-tuple naming convention. For example, the second 40 Gigabit Ethernet port is numbered as 1/2. The process of changing the configuration from 40 Gigabit Ethernet to 10 Gigabit Ethernet is called *breakout* and the process of changing the configuration from 10 Gigabit Ethernet to 40 Gigabit Ethernet is called *breakin*. When you break out a 40/100 Gigabit Ethernet port into 10 Gigabit Ethernet ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the break-out ports of the second 40 Gigabit Ethernet port are numbered as 1/2/1, 1/2/2, 1/2/3, and 1/2/4.

• On the left side of Nexus 3132Q-V switches is a set of 4 SFP+ ports multiplexed to that QSFP28 port.

By default, the RCF is structured to use the QSFP28 port.



You can make 4x SFP+ ports active instead of a QSFP port for Nexus 3132Q-V switches by using the hardware profile front portmode sfp-plus command. Similarly, you can reset Nexus 3132Q-V switches to use a QSFP port instead of 4x SFP+ ports by using the hardware profile front portmode qsfp command.

• You have configured some of the ports on Nexus 3132Q-V switches to run at 10 GbE or 40/100 GbE.



You can break out the first six ports into 4x10 GbE mode by using the interface breakout module 1 port 1-6 map 10g-4x command. Similarly, you can regroup the first six QSFP+ ports from breakout configuration by using the no interface breakout module 1 port 1-6 map 10g-4x command.

- You have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.
- The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page.

How to replace a Cisco Nexus 5596 cluster switch with a Cisco Nexus 3132Q-V cluster switch

To replace an existing Nexus 5596 cluster switch with a Nexus 3132Q-V cluster switch, you must perform a specific sequence of tasks.

About this task

The examples in this procedure describe replacing Nexus 5596 switches with Nexus 3132Q-V switches. You can use these steps (with modifications) to replace other older Cisco switches. The procedure uses the following switch and node nomenclature:

- The command outputs might vary depending on different releases of ONTAP.
- The Nexus 5596 switches to be replaced are CL1 and CL2.
- The Nexus 3132Q-V switches to replace the Nexus 5596 switches are C1 and C2.
- n1_clus1 is the first cluster logical interface (LIF) connected to cluster switch 1 (CL1 or C1) for node n1.
- n1_clus2 is the first cluster LIF connected to cluster switch 2 (CL2 or C2) for node n1.
- n1 clus3 is the second LIF connected to cluster switch 2 (CL2 or C2) for node n1.
- n1 clus4 is the second LIF connected to cluster switch 1 (CL1 or C1) for node n1.
- The nodes are n1, n2, n3, and n4.
- The examples in this procedure use four nodes: Two nodes use four 10 GbE cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40/100 GbE cluster interconnect ports: e4a, e4e. The Hardware Universe lists the actual cluster ports on your platforms.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

This procedure covers the following scenarios:

- The cluster starts with two nodes connected and functioning in a 2 Nexus 5596 cluster switches.
- The cluster switch CL2 to be replaced by C2 (Steps 1 19)
 - Traffic on all cluster ports and LIFs on all nodes connected to CL2 are migrated onto the first cluster ports and LIFs connected to CL1.
 - Disconnect cabling from all cluster ports on all nodes connected to CL2, and then use supported breakout cabling to reconnect the ports to new cluster switch C2.
 - Disconnect cabling between ISL ports between CL1 and CL2, and then use supported break-out cabling to reconnect the ports from CL1 to C2.
 - Traffic on all cluster ports and LIFs connected to C2 on all nodes is reverted.
- The cluster switch CL2 to be replaced by C2 (Steps 20 33)
 - Traffic on all cluster ports or LIFs on all nodes connected to CL1 are migrated onto the second cluster ports or LIFs connected to C2.
 - Disconnect cabling from all cluster port on all nodes connected to CL1 and reconnect, using supported break-out cabling, to new cluster switch C1.
 - Disconnect cabling between ISL ports between CL1 and C2, and reconnect using supported cabling, from C1 to C2.
 - Traffic on all cluster ports or LIFs connected to C1 on all nodes is reverted.
- Two FAS9000 nodes have been added to cluster with examples showing cluster details (Steps 34 37).

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh

x is the duration of the maintenance window in hours.



The message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Display information about the devices in your configuration:

network device-discovery show

The following example shows how many cluster interconnect interfaces have been configured in each node for each cluster interconnect switch:

cluster::>		device-discovery sl Discovered	low	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e0a	CL1	Ethernet1/1	N5K-C5596UP
	e0b	CL2	Ethernet1/1	N5K-C5596UP
	e0c	CL2	Ethernet1/2	N5K-C5596UP
	e0d	CL1	Ethernet1/2	N5K-C5596UP
n2	/cdp			
	e0a	CL1	Ethernet1/3	N5K-C5596UP
	e0b	CL2	Ethernet1/3	N5K-C5596UP
	e0c	CL2	Ethernet1/4	N5K-C5596UP
	e0d	CL1	Ethernet1/4	N5K-C5596UP
8 entries v	were disp	played.		

- 3. Determine the administrative or operational status for each cluster interface:
 - a. Display the network port attributes:

network port show

The following example displays the network port attributes on a system:

Node: n1	k port show)						
Node: III							
Ignore						Speed (Mbps)	Health
Health							
Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
 e0a	 Cluster	Cluster		up	9000	auto/10000	-
- e0b	Cluster	Cluster		up	9000	auto/10000	_
- -	Cluster	Cluster		up	9000	auto/10000	_
-	Clustel	Clustel		ир	3000	auco/10000	
e0d -	Cluster	Cluster		up	9000	auto/10000	-
Node: n2							
Ignore						Crood (March	II.a.l+b
Health						Speed (Mbps)	пеатип
Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a -	Cluster	Cluster		up	9000	auto/10000	_
=0b	Cluster	Cluster		up	9000	auto/10000	_
- e0c	Cluster	Cluster		up	9000	auto/10000	_
_							

b. Display information about the logical interfaces:

network interface show

The following example displays the general information about all of the LIFs on your system:

		nterface sho			
~ .	_	Logical	Status	Network	Current
Current	_	T., + 6	7) -1	7 -1-1/261-	NT1 -
			Admin/Oper	Address/Mask	Noae
Port	HOM	e			
		_			
Cluster		_			
CIUSCCI		n1 clus1	מנו/מנו	10.10.0.1/24	n1
e0a	tru	_	α _[, α _[
			up/up	10.10.0.2/24	n1
e0b	tru	_			
		n1_clus3	up/up	10.10.0.3/24	n1
e0c	tru	е			
		n1_clus4	up/up	10.10.0.4/24	n1
e0d	tru	е			
		n2_clus1	up/up	10.10.0.5/24	n2
e0a	tru				
		n2_clus2	up/up	10.10.0.6/24	n2
e0b	tru				
		_	up/up	10.10.0.7/24	n2
e0c	tru		,	10 10 0 0 0	
		n2_clus4	up/up	10.10.0.8/24	n2

c. Display information about the discovered cluster switches:

system cluster-switch show

The following example displays the cluster switches that are known to the cluster, along with their management IP addresses:

```
cluster::*> system cluster-switch show
Switch
                              Type
                                                 Address
Model
CL1
                              cluster-network 10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
                            cluster-network 10.10.1.102
CL2
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
2 entries were displayed.
```

4. Set the -auto-revert parameter to false on cluster LIFs clus1 and clus2 on both nodes:

network interface modify

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```

5. Verify that the appropriate RCF and image are installed on the new 3132Q-V switches as necessary for your requirements, and make the essential site customizations, such as users and passwords, network addresses, and so on.

You must prepare both switches at this time. If you need to upgrade the RCF and image, follow these

steps:

- a. Go to the Cisco Ethernet Switches page on the NetApp Support Site.
- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of the RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software.

See the ONTAP 8.x or later Cluster and Management Network Switch Reference Configuration Files Download page, and then click the appropriate version.

To find the correct version, see the ONTAP 8.x or later Cluster Network Switch Download page.

6. Migrate the LIFs associated with the second Nexus 5596 switch to be replaced:

```
network interface migrate
```

The following example shows n1 and n2, but LIF migration must be done on all of the nodes:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

7. Verify the cluster's health:

```
network interface show
```

The following example shows the result of the previous network interface migrate command:

	network in nterface sh		w -role cluster		
	Logical	Status	Network	Current	
Current Is			,		
	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
	_				
Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true	-1 -12		10 10 0 2/24	n1	- 0 -
false	ni_ciusz	up/up	10.10.0.2/24	UT	e0a
14150	n1 clus3	up/up	10.10.0.3/24	n1	e0d
false	_				
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true	n2 clus1	up/up	10.10.0.5/24	n2	e0a
true	IIZ_CIUSI	up/up	10.10.0.3/24	112	eua
	n2_clus2	up/up	10.10.0.6/24	n2	e0a
false					
6.1	n2_clus3	up/up	10.10.0.7/24	n2	e0d
false	n2 clus/	11n/11n	10.10.0.8/24	n2	e0d
true	112_C1434	αρ/ αρ	10.10.0.0/24	112	Cou
8 entries w	ere display	ed.			

8. Shut down the cluster interconnect ports that are physically connected to switch CL2:

```
network port modify
```

The following commands shut down the specified ports on n1 and n2, but the ports must be shut down on all nodes:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Ping the remote cluster interfaces and perform an RPC server check:

```
cluster ping-cluster
```

The following example shows how to ping the remote cluster interfaces:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                    e0b 10.10.0.2
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
   Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
   Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.2 to Remote 10.10.0.5
   Local 10.10.0.2 to Remote 10.10.0.6
   Local 10.10.0.2 to Remote 10.10.0.7
   Local 10.10.0.2 to Remote 10.10.0.8
   Local 10.10.0.3 to Remote 10.10.0.5
   Local 10.10.0.3 to Remote 10.10.0.6
   Local 10.10.0.3 to Remote 10.10.0.7
   Local 10.10.0.3 to Remote 10.10.0.8
   Local 10.10.0.4 to Remote 10.10.0.5
   Local 10.10.0.4 to Remote 10.10.0.6
   Local 10.10.0.4 to Remote 10.10.0.7
   Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check
```

10. Shut down the ISL ports 41 through 48 on the active Nexus 5596 switch CL1:

The following example shows how to shut down ISL ports 41 through 48 on the Nexus 5596 switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface e1/41-48
(CL1) (config-if-range) # shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

If you are replacing a Nexus 5010 or 5020, specify the appropriate port numbers for ISL from page 1.

11. Build a temporary ISL between CL1 and C2.

The following example shows a temporary ISL being set up between CL1 and C2:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

12. On all nodes, remove all cables attached to the Nexus 5596 switch CL2.

With supported cabling, reconnect disconnected ports on all nodes to the Nexus 3132Q-V switch C2.

13. Remove all the cables from the Nexus 5596 switch CL2.

Attach the appropriate Cisco QSFP to SFP+ break-out cables connecting port 1/24 on the new Cisco 3132Q-V switch, C2, to ports 45 to 48 on existing Nexus 5596, CL1.

- 14. Verify that interfaces eth1/45-48 already have channel-group 1 mode active in their running configuration.
- 15. Bring up ISLs ports 45 through 48 on the active Nexus 5596 switch CL1.

The following example shows ISLs ports 45 through 48 being brought up:

```
(CL1) # configure
(CL1) (Config) # interface e1/45-48
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

16. Verify that the ISLs are up on the Nexus 5596 switch CL1:

```
show port-channel summary
```

Ports eth1/45 through eth1/48 should indicate (P) meaning that the ISL ports are up in the port-channel:

17. Verify that the ISLs are up on the 3132Q-V switch C2:

```
show port-channel summary
```

Ports eth1/24/1, eth1/24/2, eth1/24/3, and eth1/24/4 should indicate (P) meaning that the ISL ports are up in the port-channel:

```
C2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
     s - Suspended r - Module-removed
     S - Switched
                 R - Routed
     U - Up (port-channel)
     M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
    Channel
    Pol(SU)
             Eth LACP
                           Eth1/31(D) Eth1/32(D)
2 Po2(SU) Eth LACP Eth1/24/1(P) Eth1/24/2(P)
Eth1/24/3(P)
                            Eth1/24/4(P)
```

18. On all nodes, bring up all the cluster interconnect ports connected to the 3132Q-V switch C2:

```
network port modify
```

The following example shows the specified ports being brought up on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

19. On all nodes, revert all of the migrated cluster interconnect LIFs connected to C2:

```
network interface revert
```

The following example shows the migrated cluster LIFs being reverted to their home ports on nodes n1 and n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

20. Verify all the cluster interconnect ports are now reverted to their home:

```
network interface show
```

The following example shows that the LIFs on clus2 reverted to their home ports and shows that the LIFs are successfully reverted if the ports in the Current Port column have a status of true in the Is Home column. If the Is Home value is false, the LIF has not been reverted.

(HCCWOIK III	terface sho	Status	Network	Current	
Current Is	подтеат	Scacus	NCCWOLK	Cullenc	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster	-				
CIUSCCI	n1 clus1	up/up	10.10.0.1/24	n1	e0a
true	_				
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true	n1 clus3	up/up	10.10.0.3/24	n1	e0c
true	III_CIUSS	ир/ ир	10.10.0.3/24	111	600
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true					
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true	n2 clus2	up/up	10.10.0.6/24	n2	e0b
true		ω ρ / ω ρ			002
	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true	0 1 .	,	10.10.0.0/04		0.1
true	n2_clus4	up/up	10.10.0.8/24	n2	e0d

21. Verify that the clustered ports are connected:

network port show

The following example shows the result of the previous network port modify command, verifying that all the cluster interconnects are up:

```
cluster::*> network port show -role cluster
 (network port show)
Node: n1
Ignore
                                      Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster Cluster
                          up 9000 auto/10000 -
                             up 9000 auto/10000 -
e0b
      Cluster Cluster
      Cluster
                             up 9000 auto/10000 -
e0c
                Cluster
e0d Cluster Cluster up 9000 auto/10000 -
Node: n2
Ignore
                                      Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster Cluster
                         up 9000 auto/10000 -
                         up 9000 auto/10000 -
      Cluster Cluster
e0b
                             up 9000 auto/10000 -
e0c
      Cluster
                Cluster
e0d Cluster Cluster up 9000 auto/10000 -
8 entries were displayed.
```

22. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster

The following example shows how to ping the remote cluster interfaces:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                     e0b 10.10.0.2
Cluster n1 clus4 n1
                     e0d 10.10.0.4
Cluster n2 clus3 n2
                     e0c 10.10.0.7
Cluster n2_clus4 n2 e0d 10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
   Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
   Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.2 to Remote 10.10.0.5
   Local 10.10.0.2 to Remote 10.10.0.6
   Local 10.10.0.2 to Remote 10.10.0.7
   Local 10.10.0.2 to Remote 10.10.0.8
   Local 10.10.0.3 to Remote 10.10.0.5
   Local 10.10.0.3 to Remote 10.10.0.6
   Local 10.10.0.3 to Remote 10.10.0.7
   Local 10.10.0.3 to Remote 10.10.0.8
   Local 10.10.0.4 to Remote 10.10.0.5
   Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

23. On each node in the cluster, migrate the interfaces associated with the first Nexus 5596 switch, CL1, to be replaced:

network interface migrate

The following example shows the ports or LIFs being migrated on nodes n1 and n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

24. Verify the cluster status:

network interface show

The following example shows that the required cluster LIFs have been migrated to appropriate cluster ports hosted on cluster switch C2:

	Logical	Status	Network	Current	
Current Is					
/server Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0b
false	n1_clus2	up/up	10.10.0.2/24	n1	e0b
crue	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true	n1_clus4	up/up	10.10.0.4/24	n1	e0c
false	n2_clus1	up/up	10.10.0.5/24	n2	e0b
false	_				
	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true	n2_clus4	up/up	10.10.0.8/24	n2	e0c
false					
} entries w	ere display	ed.			

25. On all the nodes, shut down the node ports that are connected to CL1:

```
network port modify
```

The following example shows the specified ports being shut down on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

26. Shut down the ISL ports 24, 31, and 32 on the active 3132Q-V switch C2: shutdown

The following example shows how to shut down ISLs 24, 31, and 32:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if-range)# exit
C2(config-if)# exit
```

27. On all nodes, remove all cables attached to the Nexus 5596 switch CL1.

With supported cabling, reconnect disconnected ports on all nodes to the Nexus 3132Q-V switch C1.

28. Remove the QSFP breakout cable from Nexus 3132Q-V C2 ports e1/24.

Connect ports e1/31 and e1/32 on C1 to ports e1/31 and e1/32 on C2 using supported Cisco QSFP optical fiber or direct-attach cables.

29. Restore the configuration on port 24 and remove the temporary Port Channel 2 on C2.

30. Bring up ISL ports 31 and 32 on C2, the active 3132Q-V switch: no shutdown

The following example shows how to bring up ISLs 31 and 32 on the 3132Q-V switch C2:

31. Verify that the ISL connections are up on the 3132Q-V switch C2: show port-channel summary

Ports Eth1/31 and Eth1/32 should indicate (P), meaning that both the ISL ports are up in the port-channel:

32. On all nodes, bring up all the cluster interconnect ports connected to the new 3132Q-V switch C1:

```
network port modify
```

The following example shows all the cluster interconnect ports being brought up for n1 and n2 on the 3132Q-V switch C1:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

33. Verify the status of the cluster node port: network port show

The following example verifies that all cluster interconnect ports on all nodes on the new 3132Q-V switch C1 are up:

```
cluster::*> network port show -role cluster
 (network port show)
Node: n1
Ignore
                                       Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster
                Cluster
                              up 9000 auto/10000 -
e0b
      Cluster Cluster
                             up 9000 auto/10000 -
                              up 9000 auto/10000 -
e0c
      Cluster
                 Cluster
e0d Cluster Cluster up 9000 auto/10000 -
Node: n2
Ignore
                                       Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
                          up 9000 auto/10000 -
e0a Cluster Cluster
                          up 9000 auto/10000 -
      Cluster Cluster
e0b
                              up 9000 auto/10000 -
e0c
      Cluster
                 Cluster
e0d Cluster Cluster up 9000 auto/10000 -
8 entries were displayed.
```

34. On all nodes, revert the specific cluster LIFs to their home ports:

```
network interface revert
```

The following example shows the specific cluster LIFs being reverted to their home ports on nodes n1 and n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

35. Verify that the interface is home:

The following example shows the status of cluster interconnect interfaces is up and Is home for n1 and n2:

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>					
	Logical	Status	Network	Current	
Current Is					
	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
0148001	n1 clus1	up/up	10.10.0.1/24	n1	e0a
true	_				
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true					
	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true	n1 clus4	/n	10.10.0.4/24	n1	e0d
true	III_CIUS4	ир/ ир	10.10.0.4/24	111	eua
cruc	n2 clus1	up/up	10.10.0.5/24	n2	e0a
true	_				
	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true					
	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true	0 1 4		10 10 0 0/04	0	- 0 -1
true	nz_clus4	up/up	10.10.0.8/24	n2	e0d
8 entries we	ana dianlam	a d			

36. Ping the remote cluster interfaces and then perform a remote procedure call server check:

cluster ping-cluster

The following example shows how to ping the remote cluster interfaces:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                    e0b 10.10.0.2
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
   Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
   Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.2 to Remote 10.10.0.5
   Local 10.10.0.2 to Remote 10.10.0.6
   Local 10.10.0.2 to Remote 10.10.0.7
   Local 10.10.0.2 to Remote 10.10.0.8
   Local 10.10.0.3 to Remote 10.10.0.5
   Local 10.10.0.3 to Remote 10.10.0.6
   Local 10.10.0.3 to Remote 10.10.0.7
   Local 10.10.0.3 to Remote 10.10.0.8
   Local 10.10.0.4 to Remote 10.10.0.5
   Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

- 37. Expand the cluster by adding nodes to the Nexus 3132Q-V cluster switches.
- 38. Display the information about the devices in your configuration:

The following examples show nodes n3 and n4 with 40 GbE cluster ports connected to ports e1/7 and e1/8, respectively on both the Nexus 3132Q-V cluster switches, and both nodes have joined the cluster. The 40 GbE cluster interconnect ports used are e4a and e4e.

	Local	Discovered		
Node 	Port	Device	Interface	Platform
n1	/cdp	G1	D.1 .1/1/1	221200 11
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
		C2	Ethernet1/1/1	~
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V
12 entries				2

 $^{^{\}circ}$ network device-discovery show

[°] network port show -role cluster

[°] network interface show -role cluster

[°] system cluster-switch show

e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d	Cluster	Cluster		up	9000	auto/10000	-
Node: n2							
Ignore							
Health						Speed (Mbps)	Health
Port Status	IPspace	Broadcast D	omain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	-
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d	Cluster	Cluster		up	9000	auto/10000	-
Node: n3							
11000. 110							
Ignore						Speed(Mbps)	Health
Health Port	IPspace	Broadcast D	omain	Link	MTU	Admin/Oper	Status
Status							
e4a -	Cluster	Cluster		up	9000	auto/40000	-
e4e -	Cluster	Cluster		up	9000	auto/40000	-
Node /							
Node: n4							
Ignore						Speed(Mbps)	Health
Health Port	IPspace	Broadcast D	omain	Link	MTU	Admin/Oper	Status
C							

Status						
e4a	Cluster	Cluster	up	9000	auto/40000	-
e4e -	Cluster	Cluster	up	9000	auto/40000	_

12 entries were displayed.

	rk interface Logical	Status	Network	Current
Current	Is			
Vserver	Interfac	e Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	-	up/up	10.10.0.2/24	n1
e0b		,	10 10 0 0 /01	1
- 0 -	_	up/up	10.10.0.3/24	n1
e0c	true	11n / 11n	10.10.0.4/24	n1
e0d	true	αρ/ αρ	10.10.0.4/24	111
Coa		מנו/מנו	10.10.0.5/24	n2
e0a	true	orp, orp		
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true	/	10 10 0 0 /04	2
0.40	_	up/up	10.10.0.9/24	n3
e4a	true	110/110	10 10 0 10/24	n 3
e4e	true	սք/ սք	10.10.0.10/24	n3
		up/up	10.10.0.11/24	n4
e4a	true	~F,		
		up/up	10.10.0.12/24	n4
e4e	true			

cluster::*> system cluster-switch show Type Address cluster-network 10.10.1.103 NX3132V C1 Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I4(1)Version Source: CDP C2 cluster-network 10.10.1.104 NX3132V Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP cluster-network 10.10.1.101 NX5596 CL1 Serial Number: 01234567 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.1(1)N1(1) Version Source: CDP cluster-network 10.10.1.102 NX5596 CL2 Serial Number: 01234568 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.1(1)N1(1) Version Source: CDP 4 entries were displayed.

^{39.} Remove the replaced Nexus 5596 if they are not automatically removed: system cluster-switch delete

The following example shows how to remove the Nexus 5596:

```
cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2
```

40. Configure clusters clus1 and clus2 to auto revert on each node and confirm:

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert true
```

41. Verify that the proper cluster switches are monitored: system cluster-switch show

```
cluster::> system cluster-switch show
Switch
                                             Address
                                                              Model
                           Type
C1
                           cluster-network 10.10.1.103 NX3132V
     Serial Number: FOX000001
     Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3)14(1)
    Version Source: CDP
C2
                           cluster-network 10.10.1.104 NX3132V
     Serial Number: FOX000002
      Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3)I4(1)
    Version Source: CDP
2 entries were displayed.
```

42. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

```
system cluster-switch log setup-password
system cluster-switch log enable-collection
```

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
**RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

43. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Related information

Cisco Ethernet Switch description page

Hardware Universe

Replace CN1610 cluster switches with Cisco Nexus 3132Q-V cluster switches

You must be aware of certain configuration information, port connections, and cabling requirements when you replace CN1610 cluster switches with Cisco Nexus 3132Q-V cluster switches.

- The following cluster switches are supported:
 - NetApp CN1610
 - Cisco Nexus 3132Q-V
- The cluster switches support the following node connections:
 - NetApp CN1610: ports 0/1 through 0/12 (10 GbE)
 - Cisco Nexus 3132Q-V: ports e1/1-30 (40/100 GbE)
- The cluster switches use the following inter-switch link (ISL) ports:
 - NetApp CN1610: ports 0/13 through 0/16 (10 GbE)
 - Cisco Nexus 3132Q-V: ports e1/31-32 (40/100 GbE)
- The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
 - Nodes with 10 GbE cluster connections require QSFP to SFP+ optical fiber breakout cables or QSFP to SFP+ copper breakout cables
 - Nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28 optical modules with optical fiber cables or QSFP/QSFP28 copper direct-attach cables
- The appropriate ISL cabling is as follows:
 - Beginning: For CN1610 to CN1610 (SFP+ to SFP+), four SFP+ optical fiber or copper direct-attach cables
 - Interim: For CN1610 to Nexus 3132Q-V (QSFP to four SFP+ breakout), one QSFP to SFP+ optical fiber or copper breakout cable
 - Final: For Nexus 3132Q-V to Nexus 3132Q-V (QSFP28 to QSFP28), two QSFP28 optical fiber or copper direct-attach cables
- NetApp twinax cables are not compatible with Cisco Nexus 3132Q-V switches.

If your current CN1610 configuration uses NetApp twinax cables for cluster-node-to-switch connections or ISL connections and you want to continue using twinax in your environment, you need to procure Cisco twinax cables. Alternatively, you can use optical fiber cables for both the ISL connections and the cluster-node-to-switch connections.

 On Nexus 3132Q-V switches, you can operate QSFP/QSFP28 ports as either 40/100 Gb Ethernet or 4x 10 Gb Ethernet modes.

By default, there are 32 ports in the 40/100 Gb Ethernet mode. These 40 Gb Ethernet ports are numbered

in a 2-tuple naming convention. For example, the second 40 Gb Ethernet port is numbered as 1/2. The process of changing the configuration from 40 Gb Ethernet to 10 Gb Ethernet is called *breakout* and the process of changing the configuration from 10 Gb Ethernet to 40 Gb Ethernet is called *breakin*. When you break out a 40/100 Gb Ethernet port into 10 Gb Ethernet ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40 Gb Ethernet port are numbered as 1/2/1, 1/2/2, 1/2/3, and 1/2/4.

• On the left side of Nexus 3132Q-V switches is a set of four SFP+ ports multiplexed to the first QSFP port.

By default, the reference configuration file (RCF) is structured to use the first QSFP port.

You can make four SFP+ ports active instead of a QSFP port for Nexus 3132Q-V switches by using the hardware profile front portmode sfp-plus command. Similarly, you can reset Nexus 3132Q-V switches to use a QSFP port instead of four SFP+ ports by using the hardware profile front portmode qsfp command.



When you use the first four SFP+ ports, it will disable the first 40GbE QSFP port.

You must have configured some of the ports on Nexus 3132Q-V switches to run at 10 GbE or 40/100 GbE.

You can break out the first six ports into 4x 10 GbE mode by using the interface breakout module 1 port 1-6 map 10g-4x command. Similarly, you can regroup the first six QSFP+ ports from breakout configuration by using the no interface breakout module 1 port 1-6 map 10g-4x command.

- You must have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.
- The ONTAP and NX-OS versions that are supported in this procedure are listed on the Cisco Ethernet Switches page.
- The ONTAP and FASTPATH versions that are supported in this procedure are listed on the NetApp CN1601 and CN1610 Switches page.

How to replace CN1610 cluster switches with Cisco Nexus 3132Q-V cluster switches

To replace the existing CN1610 cluster switches in a cluster with Cisco Nexus 3132Q-V cluster switches, you must perform a specific sequence of tasks.

About this task

The examples in this procedure use four nodes: Two nodes use four 10 GbE cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40/100 GbE cluster interconnect fiber cables: e4a and e4e. The Hardware Universe has information about the cluster fiber cables on your platforms.

The examples in this procedure use the following switch and node nomenclature:

- The command outputs might vary depending on different releases of ONTAP software.
- The CN1610 switches to be replaced are CL1 and CL2.
- The Nexus 3132Q-V switches to replace the CN1610 switches are C1 and C2.
- n1_clus1 is the first cluster logical interface (LIF) that is connected to cluster switch 1 (CL1 or C1) for node n1.
- n1 clus2 is the first cluster LIF that is connected to cluster switch 2 (CL2 or C2) for node n1.

- n1 clus3 is the second LIF that is connected to cluster switch 2 (CL2 or C2) for node n1.
- n1_clus4 is the second LIF that is connected to cluster switch 1 (CL1 or C1) for node n1. The nodes are n1, n2, n3, and n4.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.

This procedure covers the following scenario:

- The cluster starts with two nodes connected to two CN1610 cluster switches.
- Cluster switch CL2 to be replaced by C2 (Steps 2 22)
 - Traffic on all cluster ports and LIFs on all nodes connected to CL2 are migrated onto the first cluster ports and LIFs connected to CL1.
 - Disconnect cabling from all cluster ports on all nodes connected to CL2, and then use supported breakout cabling to reconnect the ports to new cluster switch C2.
 - Disconnect cabling between ISL ports CL1 and CL2, and then use supported breakout cabling to reconnect the ports from CL1 to C2.
 - Traffic on all cluster ports and LIFs connected to C2 on all nodes is reverted.
- Cluster switch CL1 to be replaced by C1 (Steps 23 43)
 - Traffic on all cluster ports and LIFs on all nodes connected to CL1 are migrated onto the second cluster ports and LIFs connected to C2.
 - Disconnect cabling from all cluster ports on all nodes connected to CL1, and then use supported breakout cabling to reconnect the ports to new cluster switch C1.
 - Disconnect cabling between ISL ports CL1 and C2, and then use supported breakout cabling to reconnect the ports from C1 to C2.
 - Traffic on all migrated cluster ports and LIFs connected to C1 on all nodes is reverted.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Display information about the devices in your configuration: network device-discovery show

The following example displays how many cluster interconnect interfaces have been configured in each node for each cluster interconnect switch:

	Local	Discovered		
Node	Port	Device	Interface	Platform
n1	 /cdp			
	e0a	CL1	0/1	CN1610
	e0b	CL2	0/1	CN1610
	e0c	CL2	0/2	CN1610
	e0d	CL1	0/2	CN1610
n2	/cdp			
	e0a	CL1	0/3	CN1610
	e0b	CL2	0/3	CN1610
	e0c	CL2	0/4	CN1610
	e0d	CL1	0/4	CN1610

- 3. Determine the administrative or operational status for each cluster interface.
 - a. Display the cluster network port attributes: network port show

The following example displays the network port attributes on a system:

cluste		work port sl port show)	now -r	ole cl	uster		
Node:	n1						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	Health
Status	5						
e0a	cluster	cluster	up	9000	auto/10000	-	-
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	_
e0d	cluster	cluster	up	9000	auto/10000	-	_
Node:	n2						
		Broadcast			Speed (Mbps)		_
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	Health
Status	5						
e0a	cluster	cluster	up	9000	auto/10000	-	_
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-
8 ent	ries were (displayed.					

b. Display information about the logical interfaces: network interface show

The following example displays the general information about all of the LIFs on your system:

		interface s	how -role clust	er		
Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node		Is Home
Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	true
8 entrie	s were disp	layed.				

C. Display information about the discovered cluster switches : system cluster-switch show

The following example displays the cluster switches that are known to the cluster, along with their management IP addresses:

Switch	Туре	Address	Model
 CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

4. Set the -auto-revert parameter to false on cluster LIFs clus1 and clus4 on both nodes: network interface modify

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert false
```

5. Verify that the appropriate RCF and image are installed on the new 3132Q-V switches as necessary for your requirements, and make any essential site customizations, such as users and passwords, network addresses, and so on.

You must prepare both switches at this time. If you need to upgrade the RCF and image, follow these steps:

- a. See the Cisco Ethernet Switches page on NetApp Support Site.
- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of the RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software.

Cisco® Cluster and Management Network Switch Reference Configuration File Download

6. Migrate the LIFs associated with the second CN1610 switch to be replaced: network interface migrate



You must migrate the cluster LIFs from a connection to the node, either through the service processor or node management interface, which owns the cluster LIF being migrated.

The following example shows n1 and n2, but LIF migration must be done on all the nodes:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-destination-node n2 -destination-port e0d
```

7. Verify the cluster's health: network interface show

The following example shows the result of the previous network interface migrate command:

```
cluster::*> network interface show -role cluster
     (network interface show)
      Logical
                                  Current Current Is
              Status Network
Vserver Interface Admin/Oper Address/Mask Node
                                          Port
                                                 Home
Cluster
      n1 clus1 up/up
                       10.10.0.1/24
                                         e0a
                                   n1
                                                true
      n1 clus2 up/up
                       10.10.0.2/24
                                   n1
                                         e0a
                                                 false
      n1 clus3 up/up
                      10.10.0.3/24
                                   n1
                                         e0d
                                                false
      n1 clus4 up/up
                       10.10.0.4/24
                                         e0d
                                   n1
                                                true
      n2 clus1 up/up
                       10.10.0.5/24
                                   n2
                                         e0a
                                                true
      n2_clus2 up/up
                       10.10.0.6/24
                                   n2
                                         e0a
                                                 false
      n2 clus3 up/up
                      10.10.0.7/24
                                   n2
                                         e0d
                                                 false
      n2 clus4 up/up
                       10.10.0.8/24
                                         e0d
                                   n2
                                                 true
8 entries were displayed.
```

8. Shut down the cluster interconnect ports that are physically connected to switch CL2: network port modify

The following commands shut down the specified ports on n1 and n2, but the ports must be shut down on all nodes:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Ping the remote cluster interfaces, and then perform a remote procedure call server check: cluster ping-cluster

The following example shows how to ping the remote cluster interfaces:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1
                        e0a 10.10.0.1
Cluster n1 clus2 n1
                        e0b
                               10.10.0.2
Cluster n1 clus3 n1
                         e0c 10.10.0.3
                               10.10.0.4
Cluster n1 clus4 n1
                        e0d
Cluster n2 clus1 n2
                         e0a 10.10.0.5
Cluster n2 clus2 n2
                        e0b
                               10.10.0.6
Cluster n2 clus3 n2
                        e0c
                               10.10.0.7
Cluster n2 clus4 n2
                         e0d
                                10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
   Local 10.10.0.3 to Remote 10.10.0.5
   Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
   Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

10. Shut down the ISL ports 13 through 16 on the active CN1610 switch CL1: shutdown

The following example shows how to shut down ISL ports 13 through 16 on the CN1610 switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface 0/13-0/16
(CL1) (Interface 0/13-0/16) # shutdown
(CL1) (Interface 0/13-0/16) # exit
(CL1) (Config) # exit
(CL1) #
```

11. Build a temporary ISL between CL1 and C2:

The following example builds a temporary ISL between CL1 (ports 13-16) and C2 (ports e1/24/1-4):

```
C2# configure

C2(config)# interface port-channel 2

C2(config-if)# switchport mode trunk

C2(config-if)# spanning-tree port type network

C2(config-if)# mtu 9216

C2(config-if)# interface breakout module 1 port 24 map 10g-4x

C2(config)# interface e1/24/1-4

C2(config-if-range)# switchport mode trunk

C2(config-if-range)# mtu 9216

C2(config-if-range)# channel-group 2 mode active

C2(config-if-range)# exit

C2(config-if)# exit
```

12. On all nodes, remove the cables that are attached to the CN1610 switch CL2.

With supported cabling, you must reconnect the disconnected ports on all of the nodes to the Nexus 3132Q-V switch C2.

13. Remove four ISL cables from ports 13 to 16 on the CN1610 switch CL1.

You must attach appropriate Cisco QSFP to SFP+ breakout cables connecting port 1/24 on the new Cisco 3132Q-V switch C2, to ports 13 to 16 on existing CN1610 switch CL1.



When reconnecting any cables to the new Cisco 3132Q-V switch, you must use either optical fiber or Cisco twinax cables.

14. To make the ISL dynamic, configure the ISL interface 3/1 on the active CN1610 switch to disable the static mode: no port-channel static

This configuration matches with the ISL configuration on the 3132Q-V switch C2 when the ISLs are brought up on both switches in step 11

The following example shows the configuration of the ISL interface 3/1 using the no port-channel static command to make the ISL dynamic:

```
(CL1) # configure
(CL1) (Config) # interface 3/1
(CL1) (Interface 3/1) # no port-channel static
(CL1) (Interface 3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

15. Bring up ISLs 13 through 16 on the active CN1610 switch CL1.

The following example illustrates the process of bringing up ISL ports 13 through 16 on the port-channel interface 3/1:

```
(CL1) # configure

(CL1) (Config) # interface 0/13-0/16,3/1

(CL1) (Interface 0/13-0/16,3/1) # no shutdown

(CL1) (Interface 0/13-0/16,3/1) # exit

(CL1) (Config) # exit

(CL1) #
```

16. Verify that the ISLs are up on the CN1610 switch CL1: show port-channel

The "Link State" should be Up, "Type" should be Dynamic, and the "Port Active" column should be True for ports 0/13 to 0/16:

```
(CL1) # show port-channel 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr
    Device/
             Port
                    Port
Ports Timeout
             Speed
                    Active
_____
0/13 actor/long
            10 Gb Full True
   partner/long
0/14 actor/long
            10 Gb Full True
   partner/long
0/15 actor/long
            10 Gb Full True
    partner/long
0/16
    actor/long
            10 Gb Full True
    partner/long
```

17. Verify that the ISLs are up on the 3132Q-V switch C2: show port-channel summary

Ports Eth1/24/1 through Eth1/24/4 should indicate (P), meaning that all four ISL ports are up in the port-channel. Eth1/31 and Eth1/32 should indicate (D) as they are not connected:

```
C2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       S - Switched R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
Group Port-
              Type Protocol Member Ports
    Channel
1 Po1(SU) Eth LACP Eth1/31(D) Eth1/32(D)
    Po2 (SU)
              Eth LACP
                               Eth1/24/1(P) Eth1/24/2(P)
Eth1/24/3(P)
                                 Eth1/24/4(P)
```

18. Bring up all of the cluster interconnect ports that are connected to the 3132Q-V switch C2 on all of the nodes: network port modify

The following example shows how to bring up the cluster interconnect ports connected to the 3132Q-V switch C2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true cluster::*> network port modify -node n1 -port e0c -up-admin true cluster::*> network port modify -node n2 -port e0b -up-admin true cluster::*> network port modify -node n2 -port e0c -up-admin true
```

19. Revert all of the migrated cluster interconnect LIFs that are connected to C2 on all of the nodes: network interface revert

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
```

20. Verify that all of the cluster interconnect ports are reverted to their home ports: network interface

show

The following example shows that the LIFs on clus2 are reverted to their home ports, and shows that the LIFs are successfully reverted if the ports in the "Current Port" column have a status of true in the "Is Home" column. If the Is Home value is false, then the LIF is not reverted.

cluster::*> network interface show -role cluster (network interface show) Logical Status Network Current Current Is Interface Admin/Oper Address/Mask Cluster n1 clus1 up/up 10.10.0.1/24 e0a n1 true n1 clus2 up/up 10.10.0.2/24 n1 e0b true n1_clus3 up/up 10.10.0.3/24 n1 e0c true n1 clus4 up/up 10.10.0.4/24 n1 e0d true n2 clus1 up/up 10.10.0.5/24 n2 e0a true n2 clus2 up/up 10.10.0.6/24 n2 e0b true n2 clus3 up/up 10.10.0.7/24 n2 e0c true n2 clus4 up/up 10.10.0.8/24 n2 e0d true 8 entries were displayed.

21. Verify that all of the cluster ports are connected: network port show

The following example shows the result of the previous $network\ port\ modify\ command$, verifying that all of the cluster interconnects are up:

clust		work port show)	now -ro	le clu	ster		
Node:	n1						
		Broadcast			Speed (Mbps)		Ignore
Port Statu	-	Domain	Link	MTU	Admin/Open	Status	Health
							-
e0a	cluster	cluster	up	9000	auto/10000	_	_
e0b	cluster	cluster	up	9000	auto/10000	_	_
e0c	cluster	cluster	up	9000	auto/10000	_	_
e0d	cluster	cluster	up	9000	auto/10000	-	-
Node:	n2						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	Health
Statu	S						
							_
e0a	cluster	cluster	up	9000	auto/10000	-	-
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-
8 ent	ries were	displayed.					

22. Ping the remote cluster interfaces and then perform a remote procedure call server check: cluster ping-cluster

The following example shows how to ping the remote cluster interfaces:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1
                         e0a 10.10.0.1
Cluster n1 clus2 n1
                         e0b
                                10.10.0.2
Cluster n1 clus3 n1
                         e0c 10.10.0.3
Cluster n1 clus4 n1
                         e0d
                                10.10.0.4
Cluster n2 clus1 n2
                          e0a 10.10.0.5
Cluster n2 clus2 n2
                         e0b
                                10.10.0.6
Cluster n2 clus3 n2
                          e0c
                                10.10.0.7
Cluster n2 clus4 n2
                          e0d
                                 10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

23. On each node in the cluster, migrate the interfaces that are associated with the first CN1610 switch CL1, to be replaced: network interface migrate

The following example shows the ports or LIFs being migrated on nodes n1 and n2:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1
-source-node n1
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n1_clus4
-source-node n1
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver cluster -lif n2_clus1
-source-node n2
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n2_clus4
-source-node n2
-destination-node n2 -destination-port e0c
```

24. Verify the cluster status: network interface show

The following example shows that the required cluster LIFs have been migrated to the appropriate cluster ports hosted on cluster switch C2:

		interface serface show)	how -role clust	er		
	Logical	Status	Network	Current	Current	Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	Home
Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0b	false
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0c	false
	n2_clus1	up/up	10.10.0.5/24	n2	e0b	false
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2_clus4	up/up	10.10.0.8/24	n2	e0c	false
8 entrie	s were disp	layed.				

25. Shut down the node ports that are connected to CL1 on all of the nodes: network port modify

The following example shows how to shut down the specified ports on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

26. Shut down the ISL ports 24, 31, and 32 on the active 3132Q-V switch C2: shutdown

The following example shows how to shut down ISLs 24, 31, and 32 on the active 3132Q-V switch C2:

```
C2# configure
C2(config)# interface ethernet 1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if-range)# exit
C2(config)# exit
```

27. Remove the cables that are attached to the CN1610 switch CL1 on all of the nodes.

With supported cabling, you must reconnect the disconnected ports on all of the nodes to the Nexus 3132Q-V switch C1.

28. Remove the QSFP cables from Nexus 3132Q-V C2 port e1/24.

You must connect ports e1/31 and e1/32 on C1 to ports e1/31 and e1/32 on C2 using supported Cisco QSFP optical fiber or direct-attach cables.

29. Restore the configuration on port 24 and remove the temporary port-channel 2 on C2:

The following example copies the running-configuration file to the startup-configuration file:

30. Bring up ISL ports 31 and 32 on C2, the active 3132Q-V switch: no shutdown

The following example shows how to bring up ISLs 31 and 32 on the 3132Q-V switch C2:

31. Verify that the ISL connections are up on the 3132Q-V switch C2: show port-channel summary

Ports Eth1/31 and Eth1/32 should indicate (P), meaning that both the ISL ports are up in the port-channel.

```
C1# show port-channel summary

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

-----

Group Port Type Protocol Member Ports

Channel

1 Pol(SU) Eth LACP Eth1/31(P) Eth1/32(P)
```

32. Bring up all of the cluster interconnect ports connected to the new 3132Q-V switch C1 on all of the nodes: network port modify

The following example shows how to bring up all of the cluster interconnect ports connected to the new 3132Q-V switch C1:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

33. Verify the status of the cluster node port: network port show

The following example verifies that all of the cluster interconnect ports on n1 and n2 on the new 3132Q-V switch C1 are up:

```
cluster::*> network port show -role cluster
     (network port show)
Node: n1
                            Speed (Mbps) Health Ignore
           Broadcast
Port IPspace Domain Link MTU Admin/Open Status Health
Status
e0a cluster cluster up 9000 auto/10000
e0b cluster cluster up 9000 auto/10000
e0c cluster cluster
                   up 9000 auto/10000
e0d cluster cluster up 9000 auto/10000 -
Node: n2
           Broadcast
                            Speed (Mbps) Health Ignore
Port IPspace Domain Link MTU Admin/Open Status Health
Status
_____
e0a cluster cluster up 9000 auto/10000
e0b cluster cluster up 9000 auto/10000
eOc cluster cluster up 9000 auto/10000
e0d cluster cluster up 9000 auto/10000 -
8 entries were displayed.
```

34. Revert all of the migrated cluster interconnect LIFs that were originally connected to C1 on all of the nodes: network interface revert

The following example shows how to revert the migrated cluster LIFs to their home ports:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n1_clus4
cluster::*> network interface revert -vserver cluster -lif n2_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus4
```

35. Verify that the interface is now home: network interface show

The following example shows the status of cluster interconnect interfaces is up and Is home for n1 and n2:

Vserver Interface Admin/Oper Address/Mask Node Port Home Cluster n1 clus1 up/up 10.10.0.1/24 n1 e0a true n1_clus2 up/up 10.10.0.2/24 n1 e0b true n1 clus3 up/up 10.10.0.3/24 n1 e0c true n1 clus4 up/up 10.10.0.4/24 n1 e0d true n2_clus1 up/up 10.10.0.5/24 n2 e0a true n2 clus2 up/up 10.10.0.6/24 n2 e0b true n2 clus3 up/up 10.10.0.7/24 n2 e0c true n2 clus4 up/up 10.10.0.8/24 n2 e0d true

8 entries were displayed.

36. Ping the remote cluster interfaces and then perform a remote procedure call server check: cluster ping-cluster

The following example shows how to ping the remote cluster interfaces:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                        e0b
                               10.10.0.2
Cluster n1_clus3 n1
                        e0c 10.10.0.3
Cluster n1 clus4 n1
                        e0d
                               10.10.0.4
Cluster n2 clus1 n2
                         e0a 10.10.0.5
Cluster n2 clus2 n2
                        e0b 10.10.0.6
Cluster n2 clus3 n2
                        e0c
                               10.10.0.7
Cluster n2 clus4 n2
                         e0d
                                10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
   Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

- 37. Expand the cluster by adding nodes to the Nexus 3132Q-V cluster switches.
- 38. Display the information about the devices in your configuration:

The following examples show nodes n3 and n4 with 40 GbE cluster ports connected to ports e1/7 and e1/8, respectively on both the Nexus 3132Q-V cluster switches, and both nodes have joined the cluster. The 40 GbE cluster interconnect ports used are e4a and e4e.

		Discovered		
Node	Port	Device	Interface	Platform
1	 /cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
.3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
14	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

[°] network device-discovery show

 $^{^{\}circ}$ network port show -role cluster

[°] network interface show -role cluster

[°] system cluster-switch show

	(network	port show)					
Node:	n1						
Port Status	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Open		Ignore Health
							_
e0a	cluster	cluster	up	9000	auto/10000	-	_
e0b	cluster	cluster	up	9000	auto/10000	_	_
e0c	cluster	cluster	up	9000	auto/10000	_	_
e0d	cluster	cluster	up	9000	auto/10000	-	-
Node:	n2						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open		Health
Status	_						
							-
e0a	cluster	cluster	up	9000	auto/10000	_	_
e0b	cluster	cluster	up	9000	auto/10000	_	_
e0c	cluster	cluster	up	9000	auto/10000	_	_
e0d	cluster	cluster	up	9000	auto/10000	-	-
Node:	n3						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open		Health
Status	_				-		
							_
e4a	cluster	cluster	up	9000	auto/40000	-	-
e4e	cluster	cluster	up	9000	auto/40000	-	-
Node:	n4						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open		Health
Statu	_				•		
							-
e4a	cluster	cluster	up	9000	auto/40000	-	-
e4e	cluster	cluster	up	9000	auto/40000	-	-

12 entries were displayed.

	Logical	Status	Network	Current	Current	Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	Home
Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	true
	n3_clus1	up/up	10.10.0.9/24	n3	e4a	true
	n3_clus2	up/up	10.10.0.10/24	n3	e4e	true
	n4_clus1	up/up	10.10.0.11/24	n4	e4a	true
	n4_clus2	up/up	10.10.0.12/24	n4	e4e	true

```
cluster::> system cluster-switch show
                           Type
                                           Address Model
                          cluster-network 10.10.1.103 NX3132V
C1
     Serial Number: FOX000001
     Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3) I4(1)
   Version Source: CDP
C2
                          cluster-network 10.10.1.104 NX3132V
    Serial Number: FOX000002
     Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3) I4(1)
   Version Source: CDP
CL1
                          cluster-network 10.10.1.101 CN1610
     Serial Number: 01234567
      Is Monitored: true
           Reason:
  Software Version: 1.2.0.7
   Version Source: ISDP
CL2
                           cluster-network 10.10.1.102 CN1610
     Serial Number: 01234568
      Is Monitored: true
           Reason:
  Software Version: 1.2.0.7
   Version Source: ISDP
4 entries were displayed.
```

39. Remove the replaced CN1610 switches if they are not automatically removed: system cluster-switch delete

The following example shows how to remove the CN1610 switches:

```
cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2
```

40. Configure clusters clus1 and clus4 to -auto-revert on each node and confirm:

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert true
```

41. Verify that the proper cluster switches are monitored: system cluster-switch show

```
cluster::> system cluster-switch show
Switch
                           Type
                                             Address
                                                               Model
C1
                           cluster-network 10.10.1.103 NX3132V
     Serial Number: FOX000001
      Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3)I4(1)
    Version Source: CDP
C2
                           cluster-network 10.10.1.104 NX3132V
     Serial Number: FOX000002
      Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3)I4(1)
    Version Source: CDP
2 entries were displayed.
```

42. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

system cluster-switch log setup-password
system cluster-switch log enable-collection

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```

If any of these commands return an error, contact NetApp support.

43. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Related information

NetApp CN1601 and CN1610 description page

Cisco Ethernet Switch description page

Hardware Universe

Cisco Nexus 3232C switches

Cisco Nexus 3232C switches

You can use Cisco Nexus 3232C switches as cluster switches in your AFF or FAS cluster.

Overview

- You can install the switch, migrate from an existing switch, replace a switch, and update the RCF files on the switch.
- You can install NX-OS and reference configuration files (RCF's) on the Cisco Nexus 3232C cluster switch.
- You can migrate from a two-node switchless cluster to a cluster with Cisco Nexus 3232C cluster switches.
- You can replace a Cisco Nexus 3232C cluster or storage switch.
- You can install the Cisco Nexus 3232C switch (X190100) NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

Available documentation

The following table lists the documentation available for the Cisco Nexus 3232C switches.

Title	Description
Install a Cisco® Nexus 3232C cluster switch and pass-through panel in a NetApp® cabinet	Describes how to install the pass-through panel in system cabinets where power connectors are at the front of the chassis and power distribution units are located in the rear of the chassis.
Setup the Cisco® Nexus 3232C cluster switches	Describes how to setup and configure your Cisco Nexus 3232C cluster switches.
Install NX-OS and Reference Configuration Files (RCFs)	Describes how to install NX-OS and reference configuration files (RCFs) on Nexus 3232C cluster switch.
Migrate from a Cisco Nexus 5596 Switch to a Cisco Nexus 3232C Switch	Describes how to migrate from environments that use older Cisco switches to environments that use Cisco 3232C switches.
Migrate from a CN1610 Switch to a Cisco Nexus 3232C Switch	Describes the procedure to replace a CN1610 switch with a Cisco Nexus 3232C cluster switch.
Migrate from a two-node Switchless Cluster	Describes how to migrate from a two-node switchless cluster environment to a two-node switched environment using Cisco Nexus 3232C cluster switches.

Replace a Cisco Nexus 3232C Cluster Switch	Describes the procedure to replace a defective Cisco Nexus 3232C switch in a cluster and download the switch operating system and reference configuration file.
Replace a Cisco Nexus 3232C Storage Switch	Describes the procedure to replace a defective Cisco Nexus 3232C storage switch and download the switch operating system and reference configuration file.

Install a Cisco Nexus 3232C cluster switch and a passthrough panel in a NetApp cabinet

You can install the Cisco Nexus 3232C switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.

Before you begin

You must have reviewed the initial preparation requirements, kit contents, and safety precautions in the Cisco Nexus 3000 Series Hardware Installation Guide.

About this task

- Fo- each switch, you must supply the eight 10-32 or 12-24 screws and clip nuts to mount the brackets and slider rails to the front and rear cabinet posts.
- You must use the Cisco standard rail kit to install the switch in a NetApp cabinet.



The jumper cords are not included with the pass-through kit and should be included with your switches. If they were not shipped with the switches, you can order them from NetApp (part number X1558A-R6).

Steps

1. Install the pass-through blanking panel in the NetApp cabinet.

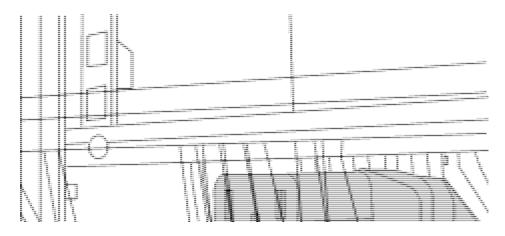
The pass-through panel kit is available from NetApp (part number X8784-R6).

The NetApp pass-through panel kit contains the following hardware:

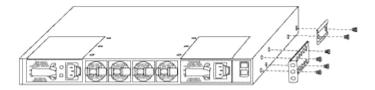
- One pass-through blanking panel
- Four 10-32 x .75 screws
- Four 10-32 clip nuts
 - a. Determine the vertical location of the switches and blanking panel in the cabinet.

In this procedure, the blanking panel will be installed in U40.

- b. Install two clip nuts on each side in the appropriate square holes for front cabinet rails.
- c. Center the panel vertically to prevent intrusion into adjacent rack space, and then tighten the screws.
- d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



- 1. Female connector of the jumper cord.
- 2. Install the rack-mount brackets on the Nexus 3232C switch chassis.
 - a. Position a front rack-mount bracket on one side of the switch chassis so that the mounting ear is aligned with the chassis faceplate (on the PSU or fan side), and then use four M4 screws to attach the bracket to the chassis.



- b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.
- c. Install the rear rack-mount bracket on the switch chassis.
- d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.
- 3. Install the clip nuts in the square hole locations for all four IEA posts.



The two 3232C switches will always be mounted in the top 2U of the cabinet RU41 and 42.

- 4. Install the slider rails in the cabinet.
 - a. Position the first slider rail at the RU42 mark on the back side of the rear left post, insert screws with the matching thread type, and then tighten the screws with your fingers.



- 1. As you gently slide the slider rail, align it to the screw holes in the rack.
- 2. Tighten the screws of the slider rails to the cabinet posts.
- b. Repeat step 4a for the right side rear post.

- c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.
- 5. Install the switch in the cabinet.



This step requires two people: one person to support the switch from the front and another to guide the switch into the rear slider rails.

a. Position the back of the switch at RU41.



- 1. As the chassis is pushed toward the rear posts, align the two rear rack-mount guides with the slider rails.
- 2. Gently slide the switch until the front rack-mount brackets are flush with the front posts.
- b. Attach the switch to the cabinet.



- 1. With one person holding the front of the chassis level, the other person should fully tighten the four rear screws to the cabinet posts.
- c. With the chassis now supported without assistance, fully tighten the front screws to the posts.
- d. Repeat steps 5a through 5c for the second switch at the RU42 location.



By using the fully installed switch as a support, it is not necessary to hold the front of the second switch during the installation process.

- 6. When the switches are installed, connect the jumper cords to the switch power inlets.
- 7. Connect the male plugs of both jumper cords to the closest available PDU outlets.



To maintain redundancy, the two cords must be connected to different PDUs.

8. Connect the management port on each 3232C switch to either of the management switches (if ordered) or connect them directly to your management network.

The management port is the upper-right port located on the PSU side of the switch. The CAT6 cable for each switch needs to be routed through the pass-through panel after the switches are installed to connect to the management switches or management network.

Set up

Set up the switches

If you do not already have the required configuration information and documentation, you need to gather that information before setting up your cluster and management network switches.

- You must have access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- You must have the required cluster network and management network switch documentation.

See Required documentation for more information.

• You must have the required controller documentation and ONTAP documentation.

NetApp documentation

- You must have the applicable licenses, network and configuration information, and cables.
- You must have the completed cabling worksheets.



Due to the complexity that can result from illustrating layers of cabling, this guide does not provide cabling graphics. This guide does provide sample worksheets with recommended port assignments and blank worksheets that you can use to set up your cluster.



For more information refer to the Hardware Universe.

 All Cisco cluster network and management network switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software but do not have the RCFs loaded.



You must download the applicable NetApp cluster network and management network RCFs from the NetApp Support Site at mysupport.netapp.com for the switches that you receive.

 In addition, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for the 92300YC cluster switches. See Installing the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches for details.

Steps

1. Rack the cluster network and management network switches and controllers.

If you are installing your	Then
Cisco Nexus 9336C-FX2 in a NetApp system cabinet	See the <i>Installing a Cisco Nexus</i> 9336C-FX2 cluster switch and pass-through panel in a NetApp cabinet guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3232C in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.
Cisco Nexus 5596UP/5596T in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 5596 cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.

- 2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheets.
- 3. Power on the cluster network and management network switches and controllers.
- Perform an initial configuration of the cluster network switches based on information provided in Required configuration information.
- 5. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
- 6. Check the version on the cluster network switches, and if necessary, download the NetApp-supported version of the software to the switches.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Cluster Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and the instructions from the Cisco Ethernet Switches page.

7. Check the software version on the network switches and, if necessary, download the NetApp-supported version of the software to the switches. If you have your own switches, refer to the Cisco site.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Management Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and instructions from the Cisco Ethernet Switches page.

Related information

Required cluster configuration information

Required documentation

Sample and blank cabling worksheets

Required cluster configuration information

To configure your cluster, you need the appropriate number and type of cables and cable connectors for your switches. Depending on the type of switch you are initially configuring, you need to connect to the switch console port with the included console cable; you also need to provide specific network information.

Required network information for all switches

You need the following network information for all switch configurations:

- · IP subnet for management network traffic
- · Host names and IP addresses for each of the storage system controllers and all applicable switches
- Most storage system controllers are managed through the e0M interface by connecting to the Ethernet service port (wrench icon). On AFF A800 and AFF A700 systems, the e0M interface uses a dedicated Ethernet port.

Refer to the Hardware Universe for latest information.

Required network information for Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches

For the Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches, you need to provide applicable responses to the following initial setup questions when you first boot the switch. Your site's security policy defines the responses and services to enable.

Abort Auto Provisioning and continue with normal setup? (yes/no)

Respond with yes. The default is no.

• Do you want to enforce secure password standard? (yes/no)

Respond with **yes**. The default is yes.

• Enter the password for admin:

The default password is "admin"; you must create a new, strong password. A weak password can be rejected.

Would you like to enter the basic configuration dialog? (yes/no)

Respond with **yes** at the initial configuration of the switch.

Create another login account? (yes/no)

Your answer depends on your site's policies on alternate administrators. The default is **no**.

Configure read-only SNMP community string? (yes/no)

Respond with no. The default is no.

• Configure read-write SNMP community string? (yes/no)

Respond with **no**. The default is no.

• Enter the switch name.

The switch name is limited to 63 alphanumeric characters.

• Continue with Out-of-band (mgmt0) management configuration? (yes/no)

Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip address.

Configure the default-gateway? (yes/no)

Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.

Configure advanced IP options? (yes/no)

Respond with **no**. The default is no.

• Enable the telnet service? (yes/no)

Respond with **no**. The default is no.

• Enabled SSH service? (yes/no)

Respond with **yes**. The default is yes.



SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.

- Enter the type of SSH key you want to generate (dsa/rsa/rsa1). The default is rsa.
- Enter the number of key bits (1024-2048).
- Configure the NTP server? (yes/no)

Respond with **no**. The default is no.

• Configure default interface layer (L3/L2):

Respond with **L2**. The default is L2.

Configure default switch port interface state (shut/noshut):

Respond with **noshut**. The default is noshut.

• Configure CoPP system profile (strict/moderate/lenient/dense):

Respond with **strict**. The default is strict.

• Would you like to edit the configuration? (yes/no)

You should see the new configuration at this point. Review and make any necessary changes to the

configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.

• Use this configuration and save it? (yes/no)

Respond with **yes** to save the configuration. This automatically updates the kickstart and system images.



If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

For more information about the initial configuration of your switch, see the following guides:

Cisco Nexus 9336C-FX2 Installation and Upgrade Guides

Cisco Nexus 92300YC Installation and Upgrade Guides

Cisco Nexus 5000 Series Hardware Installation Guide

Cisco Nexus 3000 Series Hardware Installation Guide

Install the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches

You can use this procedure to install the applicable configuration file for cluster switch health monitoring of Nexus 92300YC cluster switches. In ONTAP releases 9.5P7 and earlier and 9.6P2 and earlier, you must download the cluster switch health monitor configuration file separately. In ONTAP releases 9.5P8 and later, 9.6P3 and later, and 9.7 and later, the cluster switch health monitor configuration file is bundled with ONTAP.

Before you setup the switch health monitor for 92300YC cluster switches, you must ensure that the ONTAP cluster is up and running.



It is advisable to enable SSH in order to use all features available in CSHM.

- 1. Download the cluster switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the NetApp Software download page.
 - a. On the Software download page, select Switch Health Monitor Configuration Files
 - b. Select Platform = **ONTAP** and click **Go!**
 - c. On the Switch Health Monitor Configuration Files for ONTAP page, click View & Download
 - d. On the Switch Health Monitor Configuration Files for ONTAP Description page, click **Download** for the applicable cluster switch model, for example: **Cisco Nexus 92300YC**
 - e. On the End User License Agreement page, click Accept
 - f. On the Switch Health Monitor Configuration Files for ONTAP Download page, select the applicable configuration file, for example, **Cisco_Nexus_92300YC.zip**
- 2. Upload the applicable zip file to your internal web server where the IP address is X.X.X.X.

For an internal web server IP address of 192.168.2.20 and assuming a /usr/download directory exists, you can upload your zip file to your web server using scp:

```
% scp Cisco_Nexus_92300YC.zip
admin@192.168.2.20:/usr/download/Cisco_Nexus_92300YC.zip
```

3. Access the advanced mode setting from one of the ONTAP systems in the cluster, using the command setprivilege advanced:

```
cluster1::> set -privilege advanced
```

4. Run the switch health monitor configure command system cluster-switch configure-health-monitor -node * -package-url X.X.X.X/location_to_download_zip_file:

```
cluster1::> system cluster-switch configure-health-monitor -node *
-package-url 192.168.2.20/usr/download/Cisco_Nexus_92300YC.zip
```

- 5. Verify that the command output contains the text string "downloaded package processed successfully". If an error occurs, contact NetApp support.
- 6. Run the command system cluster-switch show on the ONTAP system and ensure that the cluster switches are discovered with the monitored field set to "True".

```
cluster1::> system cluster-switch show
```



If at any time you revert to an earlier version of ONTAP, you will need to install the CSHM configuration file again to enable switch health monitoring of 92300YC cluster switches.

Required documentation

You need specific switch and controller documentation to set up your ONTAP cluster.

Required documentation for cluster network switches

To set up the Cisco Nexus 9336C-FX2 and 92300YC switches, you need the following documentation from the Cisco Nexus 9000 Series Switches Support page:

Document title	Description
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.

Document title	Description
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

To set up the Cisco Nexus 3232C and 3132Q-V switches, you need the following documentation from the Cisco Nexus 3000 Series Switches Support page:

Document title	Description
Nexus 3000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 3000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 3000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.

Document title	Description	
Cisco Nexus 3000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.	
Nexus 3000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 3000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.	
Cisco Nexus 3000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.	
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 3000 series switches.	

To set up the Cisco Nexus 5596 switch, you need the following documents from Cisco Nexus 5000 Series Switches Support page:

Document title	Description
Nexus 5000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 5000 Series Switch Software Configuration Guide (choose the guide for the software you are using)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide	Provides information about how to downgrade the switch to the supported ONTAP switch software, if necessary.
Cisco Nexus 5000 Series NX-OS Command Reference Master Index	Provides an alphabetical list of all the commands supported for a specific NX-OS release.
Cisco Nexus 5000 and Nexus 2000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 5000 switches.
Nexus 5000 Series NX-OS System Message Reference	Describes troubleshooting information.

Document title	Description
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000 Series, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 5000 series switches.

Required documentation for supported ONTAP systems

To set up an ONTAP system, you need the following documents for your version of the operating system from the ONTAP 9 Documentation Center.

Name	Description
Controller-specific Installation and Setup Instructions	Describes how to install NetApp hardware.
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.
Hardware Universe	Provides NetApp hardware configuration and compatibility information.

Rail kit and cabinet documentation

To install a Cisco switch in a NetApp cabinet, see the following hardware documentation:

Name	Description	
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.	
Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet	Describes how to install a Cisco Nexus 3232C switch in a four-post NetApp cabinet.	
Installing a Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 3132Q-V switch in a four-post NetApp cabinet.	
Installing a Cisco Nexus 5596 switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 5596 switch in a NetApp cabinet.	

Considerations for using Smart Call Home

Smart Call Home monitors the hardware and software components on your network, to generate an email-based notification of critical system conditions. When an event occurs on your device, Smart Call Home raises an alert to all the recipients that are configured in your destination profile.

You must configure a cluster network switch to communicate using email with the Smart Call Home system. You can optionally set up your cluster network switch to take advantage of Cisco's embedded Smart Call Home support feature.

Before you can use Smart Call Home feature, you need to be aware of the following considerations:

- An email server must be in place.
- The switch must have IP connectivity to the email server.
- The contact name (SNMP server contact), phone number, and street address information must be configured.
- This is required to determine the origin of messages received.
- A CCO ID must be associated with an appropriate Cisco SMARTnet Service contract for your company.
- Cisco SMARTnet Service must be in place for the device to be registered.

The Cisco support site contains information about the commands to configure Smart Call Home.

Cisco support site

Sample and blank cabling worksheets

The sample cabling worksheets provide examples of recommended port assignments from the switches to the controllers. The blank worksheets provide a template that you can use in setting up your cluster.

Cisco Nexus 9336C-FX2 cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10GbE node 1	1	4x10GbE node 1
2	4x10GbE node 2	2	4x10GbE node 2
3	4x10GbE node 3	3	4x10GbE node 3
4	4x25GbE node 4	4	4x25GbE node 4
5	4x25GbE node 5	5	4x25GbE node 5
6	4x25GbE node 6	6	4x25GbE node 6

Cluster switch A		Cluster switch B	
7	4x100GbE node 7	7	4x100GbE node 7
8	4x100GbE node 8	8	4x100GbE node 8
9	4x100GbE node 9	9	4x100GbE node 9
10	4x100GbE node 10	10	4x100GbE node 10
11	4x100GbE node 11	11	4x100GbE node 11
12	4x100GbE node 12	12	4x100GbE node 12
13	4x100GbE node 13	13	4x100GbE node 13
14	4x100GbE node 14	14	4x100GbE node 14
15	4x100GbE node 15	15	4x100GbE node 15
16	4x100GbE node 16	16	4x100GbE node 16
17	4x100GbE node 17	17	4x100GbE node 17
18	4x100GbE node 18	18	4x100GbE node 18
19	4x100GbE node 19	19	4x100GbE node 19
20	4x100GbE node 20	20	4x100GbE node 20
21	4x100GbE node 21	21	4x100GbE node 21
22	4x100GbE node 22	22	4x100GbE node 22
23	4x100GbE node 23	23	4x100GbE node 23
24	4x100GbE node 24	24	4x100GbE node 24
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	

Cluster switch A		Cluster switch B	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Cisco Nexus 92300YC cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	10/25 GbE node	1	10/25 GbE node
2	10/25 GbE node	2	10/25 GbE node
3	10/25 GbE node	3	10/25 GbE node
4	10/25 GbE node	4	10/25 GbE node
5	10/25 GbE node	5	10/25 GbE node
6	10/25 GbE node	6	10/25 GbE node
7	10/25 GbE node	7	10/25 GbE node

Cluster switch A		Cluster switch	Cluster switch B	
8	10/25 GbE node	8	10/25 GbE node	
9	10/25 GbE node	9	10/25 GbE node	
10	10/25 GbE node	10	10/25 GbE node	
11	10/25 GbE node	11	10/25 GbE node	
12	10/25 GbE node	12	10/25 GbE node	
13	10/25 GbE node	13	10/25 GbE node	
14	10/25 GbE node	14	10/25 GbE node	
15	10/25 GbE node	15	10/25 GbE node	
16	10/25 GbE node	16	10/25 GbE node	
17	10/25 GbE node	17	10/25 GbE node	
18	10/25 GbE node	18	10/25 GbE node	
19	10/25 GbE node	19	10/25 GbE node	
20	10/25 GbE node	20	10/25 GbE node	
21	10/25 GbE node	21	10/25 GbE node	
22	10/25 GbE node	22	10/25 GbE node	
23	10/25 GbE node	23	10/25 GbE node	
24	10/25 GbE node	24	10/25 GbE node	
25	10/25 GbE node	25	10/25 GbE node	
26	10/25 GbE node	26	10/25 GbE node	
27	10/25 GbE node	27	10/25 GbE node	
28	10/25 GbE node	28	10/25 GbE node	
29	10/25 GbE node	29	10/25 GbE node	

Cluster switch A		Cluster switch	Cluster switch B	
30	10/25 GbE node	30	10/25 GbE node	
31	10/25 GbE node	31	10/25 GbE node	
32	10/25 GbE node	32	10/25 GbE node	
33	10/25 GbE node	33	10/25 GbE node	
34	10/25 GbE node	34	10/25 GbE node	
35	10/25 GbE node	35	10/25 GbE node	
36	10/25 GbE node	36	10/25 GbE node	
37	10/25 GbE node	37	10/25 GbE node	
38	10/25 GbE node	38	10/25 GbE node	
39	10/25 GbE node	39	10/25 GbE node	
40	10/25 GbE node	40	10/25 GbE node	
41	10/25 GbE node	41	10/25 GbE node	
42	10/25 GbE node	42	10/25 GbE node	
43	10/25 GbE node	43	10/25 GbE node	
44	10/25 GbE node	44	10/25 GbE node	
45	10/25 GbE node	45	10/25 GbE node	
46	10/25 GbE node	46	10/25 GbE node	
47	10/25 GbE node	47	10/25 GbE node	
48	10/25 GbE node	48	10/25 GbE node	
49	40/100 GbE node	49	40/100 GbE node	
50	40/100 GbE node	50	40/100 GbE node	
51	40/100 GbE node	51	40/100 GbE node	

Cluster switch A		Cluster switch B	
52	40/100 GbE node	52	40/100 GbE node
53	40/100 GbE node	53	40/100 GbE node
54	40/100 GbE node	54	40/100 GbE node
55	40/100 GbE node	55	40/100 GbE node
56	40/100 GbE node	56	40/100 GbE node
57	40/100 GbE node	57	40/100 GbE node
58	40/100 GbE node	58	40/100 GbE node
59	40/100 GbE node	59	40/100 GbE node
60	40/100 GbE node	60	40/100 GbE node
61	40/100 GbE node	61	40/100 GbE node
62	40/100 GbE node	62	40/100 GbE node
63	40/100 GbE node	63	40/100 GbE node
64	40/100 GbE node	64	40/100 GbE node
65	100 GbE ISL to switch B port 65	65	100 GbE ISL to switch A port 65
66	100 GbE ISL to switch B port 66	66	100 GbE ISL to switch A port 65

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	

Cluster switch A		Cluster switch B	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	

Cluster switch A		Cluster switch B	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	
44		44	
45		45	
46		46	

Cluster switch A		Cluster switch B	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL to switch B port 65	65	ISL to switch A port 65
66	ISL to switch B port 66	66	ISL to switch A port 66

Cisco Nexus 3232C cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling

worksheet by using the completed sample cabling worksheet as a guide. Each switch can be configured as a single 100GbE, 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G/100G node	1	4x10G/40G/100G node
2	4x10G/40G/100G node	2	4x10G/40G/100G node
3	4x10G/40G/100G node	3	4x10G/40G/100G node
4	4x10G/40G/100G node	4	4x10G/40G/100G node
5	4x10G/40G/100G node	5	4x10G/40G/100G node
6	4x10G/40G/100Gnode	6	4x10G/40G/100Gnode
7	4x10G/40G/100G node	7	4x10G/40G/100G node
8	4x10G/40G/100G node	8	4x10G/40G/100G node
9	4x10G/40G/100G node	9	4x10G/40G/100G node
10	4x10G/40G/100G node	10	4x10G/40G/100G node
11	4x10G/40G/100G node	11	4x10G/40G/100G node
12	4x10G/40G/100G node	12	4x10G/40G/100G node
13	4x10G/40G/100G node	13	4x10G/40G/100G node
14	4x10G/40G/100G node	14	4x10G/40G/100G node
15	4x10G/40G/100G node	15	4x10G/40G/100G node
16	4x10G/40G/100G node	16	4x10G/40G/100G node
17	4x10G/40G/100G node	17	4x10G/40G/100G node
18	4x10G/40G/100G node	18	4x10G/40G/100G node

Cluster switch A		Cluster switch B	
19	40G/100G node 19	19	40G/100G node 19
20	40G/100G node 20	20	40G/100G node 20
21	40G/100G node 21	21	40G/100G node 21
22	40G/100G node 22	22	40G/100G node 22
23	40G/100G node 23	23	40G/100G node 23
24	40G/100G node 24	24	40G/100G node 24
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	

Cluster switch A		Cluster switch B	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Cisco Nexus 3132Q-V cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide. Each switch can

be configured as a single 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G node	1	4x10G/40G node
2	4x10G/40G node	2	4x10G/40G node
3	4x10G/40G node	3	4x10G/40G node
4	4x10G/40G node	4	4x10G/40G node
5	4x10G/40G node	5	4x10G/40G node
6	4x10G/40G node	6	4x10G/40G node
7	4x10G/40G node	7	4x10G/40G node
8	4x10G/40G node	8	4x10G/40G node
9	4x10G/40G node	9	4x10G/40G node
10	4x10G/40G node	10	4x10G/40G node
11	4x10G/40G node	11	4x10G/40G node
12	4x10G/40G node	12	4x10G/40G node
13	4x10G/40G node	13	4x10G/40G node
14	4x10G/40G node	14	4x10G/40G node
15	4x10G/40G node	15	4x10G/40G node
16	4x10G/40G node	16	4x10G/40G node
17	4x10G/40G node	17	4x10G/40G node
18	4x10G/40G node	18	4x10G/40G node
19	40G node 19	19	40G node 19

Cluster switch A		Cluster switch B	
20	40G node 20	20	40G node 20
21	40G node 21	21	40G node 21
22	40G node 22	22	40G node 22
23	40G node 23	23	40G node 23
24	40G node 24	24	40G node 24
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	

Cluster switch A		Cluster switch B	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Cisco Nexus 5596UP and 5596T cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

Some platforms support more than one 10GbE cluster port connection per cluster interconnect switch. To support additional cluster connections, you can use ports 25 through 40, as well as ports 49 through 80 when expansion modules are installed.

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	Node port 1	1	Node port 1
2	Node port 2	2	Node port 2
3	Node port 3	3	Node port 3
4	Node port 4	4	Node port 4
5	Node port 5	5	Node port 5
6	Node port 6	6	Node port 6
7	Node port 7	7	Node port 7
8	Node port 8	8	Node port 8
9	Node port 9	9	Node port 9
10	Node port 10	10	Node port 10
11	Node port 11	11	Node port 11
12	Node port 12	12	Node port 12
13	Node port 13	13	Node port 13
14	Node port 14	14	Node port 14
15	Node port 15	15	Node port 15
16	Node port 16	16	Node port 16
17	Node port 17	17	Node port 17
18	Node port 18	18	Node port 18

Cluster switch A		Cluster switch B	
19	Node port 19	19	Node port 19
20	Node port 20	20	Node port 20
21	Node port 21	21	Node port 21
22	Node port 22	22	Node port 22
23	Node port 23	23	Node port 23
24	Node port 24	24	Node port 24
25 through 40	Reserved	25 through 40	Reserved
41	ISL to switch B port 41	41	ISL to switch A port 41
42	ISL to switch B port 42	42	ISL to switch A port 42
43	ISL to switch B port 43	43	ISL to switch A port 43
44	ISL to switch B port 44	44	ISL to switch A port 44
45	ISL to switch B port 45	45	ISL to switch A port 45
46	ISL to switch B port 46	46	ISL to switch A port 46
47	ISL to switch B port 47	47	ISL to switch A port 47
48	ISL to switch B port 48	48	ISL to switch A port 48

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.



Switch ports 1 through 24 function as 10 GbE ports. Switch ports 41 through 48 are reserved for Inter-Switch Links (ISLs).

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	

Cluster switch A	Cluster switch B	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	
11	11	
12	12	
13	13	
14	14	
15	15	
16	16	
17	17	
18	18	
19	19	
20	20	
21	21	
22	22	
23	23	

Cluster switch A		Cluster switch B	
24		24	
25 through 40	Reserved	25 through 40	Reserved
41	ISL to switch B port 41	41	ISL to switch A port 41
42	ISL to switch B port 42	42	ISL to switch A port 42
43	ISL to switch B port 43	43	ISL to switch A port 43
44	ISL to switch B port 44	44	ISL to switch A port 44
45	ISL to switch B port 45	45	ISL to switch A port 45
46	ISL to switch B port 46	46	ISL to switch A port 46
47	ISL to switch B port 47	47	ISL to switch A port 47
48	ISL to switch B port 48	48	ISL to switch A port 48

Install NX-OS software and RCFs on Cisco Nexus 3232C cluster switches

The Cisco NX-OS software and reference configuration files (RCFs) must be installed on Cisco Nexus 3232C cluster switches.

Before you begin

The following conditions must exist before you install the NX-OS software and Reference Configurations Files (RCFs) on the cluster switch:

- The cluster must be fully functioning (there should be no errors in the logs or similar -ssues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have a console connection to the switch, required when installing the RCF.
- You must have consulted the switch compatibility table on the Cisco Ethernet switch page for the supported ONTAP, NX-OS, and RCF versions.
- There can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on Cisco Nexus 3000 Series Switches.

· You must have the current RCF.

About this task

The examples in this procedure use two nodes. These nodes use two 10GbE cluster interconnect ports e0a and e0b.

See the Hardware Universe to verify the correct cluster ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are cluster1-01 and cluster1-02.
- The cluster LIF names are cluster1-01_clus1 and cluster1-01_clus2 for cluster1-01 and cluster1-02 clus1 and cluster1-02 clus2 for cluster1-02.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=x h
```

where *x* is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

3. Display how many cluster interconnect interfaces are configured in each node for each cluster interconnect switch:

network device-discovery show -protocol cdp

<pre>cluster1::*> network device-discovery show -protocol cdp</pre>									
		Discovered Device (LLDP: ChassisID) Interface Platfo							
cluster1-02/cdp									
	e0a	cs1		Eth1/2	N3K-				
C3232C									
	e0b	cs2		Eth1/2	N3K-				
C3232C									
cluster1-01/cdp									
	e0a	cs1		Eth1/1	N3K-				
C3232C									
	e0b	cs2		Eth1/1	N3K-				
C3232C									
4 entries were displayed.									

- 4. Check the administrative or operational status of each cluster interface.
 - a. Display the network port attributes:

network port show -ipspace Cluster

<pre>cluster1::*> network port show -ipspace Cluster</pre>											
Node: cluster1-02											
					Speed(Mbps)	Health					
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status					
		G1									
e0a	Cluster	Cluster	up	9000	auto/10000	nealtny					
e0b	Cluster	Cluster	up	9000	auto/10000	healthy					
Node: cluster1-01											
					Speed(Mbps)	Health					
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status					
e0a	Cluster	Cluster	up	9000	auto/10000	healthy					
e0b	Cluster	Cluster	up	9000	auto/10000	healthy					
4 entries were displayed.											

b. Display information about the LIFs:

network interface show -vserver Cluster

cluster1::*	> network interface	show -vser	ver Cluster	
	Logical	Status	Network	Current
Current Is	- 5			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port Home	е			
Cluster				
-1+1 01	cluster1-01_clus1	up/up	169.254.209.69/16	
cluster1-01	e0a true cluster1-01 clus2	110/110	160 254 40 125/16	
cluster1-01	e0b true	ир/ир	107.234.47.123/10	
	cluster1-02 clus1	up/up	169.254.47.194/16	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.19.183/16	
cluster1-02	e0b true			
4 entries we	ere displayed.			

5. Ping the remote cluster LIFs:

cluster ping-cluster -node node-name

```
cluster1::*> **cluster ping-cluster -node cluster1-02**
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01 clus1 169.254.209.69 cluster1-01
                                                           e0a
Cluster cluster1-01 clus2 169.254.49.125 cluster1-01
                                                           e0b
Cluster cluster1-02 clus1 169.254.47.194 cluster1-02
                                                           e0a
Cluster cluster1-02 clus2 169.254.19.183 cluster1-02
                                                           e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Verify that the auto-revert command is enabled on all cluster LIFs:

network interface show -vserver Cluster -fields auto-revert

```
Cluster1::*> network interface show -vserver Cluster -fields auto-revert

Logical
Vserver Interface Auto-revert

Cluster

cluster1-01_clus1 true
cluster1-01_clus2 true
cluster1-02_clus1 true
cluster1-02_clus2 true
4 entries were displayed.
```

7. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands:

```
system switch ethernet log setup-password
system switch ethernet log enable-collection
```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

8. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands:

```
system cluster-switch log setup-password
```

system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 3232C cluster switch.

Steps

1. Connect the cluster switch to the management network.

2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the NX-OS software and EPLD images to the Nexus 3232C switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.4.bin /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.4.img /bootflash/n9000-epld.9.3.4.img
/code/n9000-epld.9.3.4.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Verify the running version of the NX-OS software:

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
 BIOS: version 08.37
 NXOS: version 9.3(3)
 BIOS compile time: 01/28/2020
 NXOS image file is: bootflash://nxos.9.3.3.bin
 NXOS compile time: 12/22/2019 2:00:00 [12/22/2019 14:00:37]
Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FO??????GD
  Device name: cs2
 bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)
Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:
```

```
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

5. Install the NX-OS image.

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[############### 100% -- SUCCESS
Verifying image type.
[############### 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[################ 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[################ 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-
              Upg-Required
```

```
9.3(3)
                                                                9.3(4)
            nxos
yes
                        v08.37(01/28/2020):v08.32(10/18/2016)
     1
            bios
v08.37(01/28/2020)
                    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.
cs2#
```

6. Verify the new version of NX-OS software after the switch has rebooted: show version

cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
but not
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or

```
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 08.37
 NXOS: version 9.3(4)
 BIOS compile time: 01/28/2020
 NXOS image file is: bootflash:///nxos.9.3.4.bin
 NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]
Hardware
 cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
 Processor Board ID FO??????GD
  Device name: rtpnpi-mcc01-8200-ms-A1
 bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)
Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
  Reason: Reset due to upgrade
  System version: 9.3(3)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

7. Upgrade the EPLD image and reboot the switch.

```
cs2# show version module 1 epld
EPLD Device
                       Version
_____
MI FPGA
                        0x12
IO FPGA
                        0x11
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
Compatibility check:
Module
                Upgradable
                              Impact Reason
1
          SUP
                Yes
                              disruptive Module Upgradable
Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module Type EPLD
                       Running-Version New-Version Upg-
Required
1 SUP MI FPGA
                             0x12 0x12
0x11 0x12
                                                  No
   1 SUP IO FPGA
                                                   Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y
Proceeding to upgrade Modules.
Starting Module 1 EPLD Upgrade
Module 1: IO FPGA [Programming]: 100.00% ( 64 of 64 sectors)
Module 1 EPLD upgrade is successful.
Module Type Upgrade-Result
----- -------
  1 SUP Success
Module 1 EPLD upgrade is successful.
cs2#
```

8. After the switch reboot, log in again, upgrade the EPLD golden image and reboot the switch once again.

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module Type Upgradable Impact Reason
_____
                                -----
    1
             SUP Yes disruptive Module Upgradable
Retrieving EPLD versions.... Please wait.
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y
Proceeding to upgrade Modules.
Starting Module 1 EPLD Upgrade
Module 1: MI FPGA [Programming]: 100.00% ( 64 of
                                                64 sect
Module 1: IO FPGA [Programming]: 100.00% ( 64 of 64 sect
Module 1 EPLD upgrade is successful.
Module Type Upgrade-Result
----- -------
   1 SUP Success
EPLDs upgraded.
Module 1 EPLD upgrade is successful.
cs2#
```

9. After the switch reboot, log in to verify that the new version of EPLD loaded successfully.

```
cs2# show version module 1 epld

EPLD Device Version

MI FPGA 0x12

IO FPGA 0x12
```

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 3232C switch for the first time. You can also use this procedure to upgrade your RCF version.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are cluster1-01, cluster1-02, cluster1-03, and cluster1-04.
- The cluster LIF names are cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1, and cluster1-04_clus2.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the -se of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches: network device-discovery show

		Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
cluster1-0	1/cdp			
	e0a	cs1	Ethernet1/7	N3K-
C3232C				
	e0d	cs2	Ethernet1/7	N3K-
C3232C				
cluster1-0	2/cdp			
	e0a	cs1	Ethernet1/8	N3K-
C3232C				
	e0d	cs2	Ethernet1/8	N3K-
C3232C				
cluster1-0	3/cdp			
	e0a	cs1	Ethernet1/1/1	N3K-
C3232C				
	e0b	cs2	Ethernet1/1/1	N3K-
C3232C				
cluster1-0	4/cdp			
	e0a	cs1	Ethernet1/1/2	N3K-
C3232C				
	e0b	cs2	Ethernet1/1/2	N3K-
C3232C				

- 2. Check the administrative and operational status of each cluster port.
 - a. Verify that all the cluster ports are up with a healthy status: network port show -role cluster

Ignore Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status	Node: clu	ıster1-01						
Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status	Ignore							
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false Node: cluster1-02 Ignore Speed(Mbps) Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status	Health						Speed (Mbps)	Health
e0a Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false Node: cluster1-02 Ignore Speed(Mbps) Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status		IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false Node: cluster1-02 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0d Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status entries were Cluster up 9000 auto/100000 health false e0b Cluster Cluster up 9000 auto/100000000 health false e0b Cluster Cluster up 9000 auto/100000 health false e0b Cluster Cluster up 9000 a	Status							
healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false Node: cluster1-02 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status	 							
eod Cluster Cluster up 9000 auto/100000 healthy false Node: cluster1-02 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status	e0a	Cluster	Cluster		up	9000	auto/100000)
Node: cluster1-02 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status	_							
Node: cluster1-02 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status Cluster up 9000 auto/10000 health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health			Cluster		up	9000	auto/100000)
Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status	healthy f	talse						
Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status	Node: clu	ister1-02						
Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status	Ignore							
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	Health						Speed (Mbps)	Health
Status		IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a Cluster Cluster up 9000 auto/100000 healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status		-						
healthy false e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health								
e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	e0a	Cluster	Cluster		up	9000	auto/100000)
healthy false 8 entries were displayed. Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	healthy f	Talse						
Node: cluster1-03 Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health			Cluster		up	9000	auto/100000)
Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	_							
Ignore Speed(Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	8 entries	s were displa	yed.					
Speed (Mbps) Health Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status Cluster Cluster up 9000 auto/10000 health false Cluster Cluster up 9000 auto/10000 health	Node: clu	ister1-03						
Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	Ignore	è						
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status e0a Cluster Cluster up 9000 auto/10000 health false e0b Cluster Cluster up 9000 auto/10000 health	Health						Speed (Mbps)	неаlth
Status		IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
false eOb Cluster Cluster up 9000 auto/10000 health		•					1	
false eOb Cluster Cluster up 9000 auto/10000 health								
false eOb Cluster Cluster up 9000 auto/10000 health	 e0a	Cluster	Cluster		מוו	9000	auto/1000	health
·		CIUSCEI	CIUSCEI		uр	5000	auco/10000	iicai cii
		Cluster	Cluster		up	9000	auto/10000	health
	false							

Ignore							
						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast D	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
false							
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
false							
cluster1:	: *>						

b. Verify that all the cluster interfaces (LIFs) are on the home port:

network interface show -role cluster

		Logical	Status	Network	Current
Cur	rent Is				
Vse	rver	Interface	Admin/Open	r Address/Mask	Node
Por	t Hom	е			
	ster				
CIU	Ster	cluster1-01 clus1	un/un	169.254.3.4/23	cluster1-
01	e0a	true	αρ/αρ	107.231.3.1/23	CIUDCCII
		cluster1-01 clus2	up/up	169.254.3.5/23	cluster1-
01	e0d	true			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1
02	e0a	true			
		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1
02	e0d	true	,		
0.0	0	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1
03	e0a	true		160 054 1 1/00	cluster1
03	e0b	cluster1-03_clus2 true	up/up	169.254.1.1/23	Clusteri-
03	COD	cluster1-04 clus1	up/up	169.254.1.6/23	cluster1
04	e0a	true	αp, αp	103,1201,110,120	01400011
		cluster1-04 clus2	up/up	169.254.1.7/23	cluster1
04	e0b	true			
8 e	ntries w	ere displayed.			

c. Verify that the cluster displays information for both cluster switches:

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch
                                                              Model
                           Type
                                             Address
______
                           cluster-network 10.233.205.92
cs1
NX3232C
    Serial Number: FOXXXXXXXGS
     Is Monitored: true
           Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(4)
   Version Source: CDP
cs2
                           cluster-network 10.233.205.93
NX3232C
    Serial Number: FOXXXXXXXGD
     Is Monitored: true
           Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(4)
   Version Source: CDP
2 entries were displayed.
```

3. Disable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif \* -auto
-revert false
```

4. On cluster switch cs2, shut down the ports connected to the cluster ports of the nodes.

```
cs2(config) # interface eth1/1/1-2,eth1/7-8
cs2(config-if-range) # shutdown
```

5. Verify that the cluster ports have migrated to the ports hosted on cluster switch cs1. This might take a few seconds.

network interface show -role cluster

		Logical	Status	Network	Current
Current					_
			Admin/Oper	Address/Mask	Node
Port		e 			
Cluster		cluster1-01 clus1	up/up	169.254.3.4/23	cluster1-01
e0a	true	_			
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0a	fals	se			
		<pre>cluster1-02_clus1</pre>	up/up	169.254.3.8/23	cluster1-02
e0a	true				
		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0a	fals		,		
		cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0a	true		,	160 054 1 1/00	1 1 00
- 0 -	fals	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0a	lais	cluster1-04 clus1	11n /11n	169.254.1.6/23	cluster1-04
e0a	true	-	ир/ир	107.234.1.0/23	CIUSCEII-04
Coa	CIUC	cluster1-04 clus2	מנו/מנו	169.254.1.7/23	cluster1-04
e0a	fals	_			
		ere displayed.			

6. Verify that the cluster is healthy:

cluster show

cluster1::*> cluster	show		
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displ	ayed.		
cluster1::*>			
cluster1::*>			

- 7. Clean the configuration on switch cs2 and perform a basic setup.
 - a. Clean the configuration. This step requires a console connection to the switch.

```
cs2# write erase Warning: This command will erase the startup-configuration. Do you wish to proceed anyway? (y/n) [n] y cs2# reload This command will reboot the system. (y/n)? [n] y cs2#
```

- b. Perform a basic setup of the switch.
- 8. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference guides.

This example shows TFTP being used to copy an RCF to the bootflash on switch cs2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

9. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference guides.

This example shows the RCF file Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt being installed on switch cs2:

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-config echo-commands
```

10. Examine the banner output from the show banner motd command. You must read and follow the instructions under **Important Notes** to ensure the proper configuration and operation of the switch.

```
* Version : v1.6
* Port Usage : Breakout configuration
* Ports 1- 3: Breakout mode (4x10GbE) Intra-Cluster Ports, int e1/1/1-
4,
* e1/2/1-4, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25GbE) Intra-Cluster/HA Ports, int
e1/4/1-4,
* e1/5/1-4, e1/6/1-4
* Ports 7-30: 40/100GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
* Ports 33-34: 10GbE Intra-Cluster 10GbE Ports, int e1/33-34
* IMPORTANT NOTES
* - Load Nexus 3232C RCF v1.6-Cluster-HA.txt for non breakout config
* - This RCF utilizes QoS and requires TCAM re-configuration, requiring
RCF
  to be loaded twice with the Cluster Switch rebooted in between.
* - Perform the following 4 steps to ensure proper RCF installation:
    (1) Apply RCF first time, expect following messages:
        - Please save config and reload the system...
        - Edge port type (portfast) should only be enabled on ports...
        - TCAM region is not configured for feature QoS class IPv4
ingress...
    (2) Save running-configuration and reboot Cluster Switch
    (3) After reboot, apply same RCF second time and expect following
messages:
       - % Invalid command at '^' marker
        - Syntax error while parsing...
    (4) Save running-configuration again
******************
*****
```



When applying the RCF for the first time, the **ERROR: Failed to write VSH commands** message is expected and can be ignored.

1. Verify that the RCF file is the correct newer version:

show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is

correct:

- The RCF banner
- The node and port settings
- Customizations
 The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.
- 2. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference guides.

3. Reboot switch cs2. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs2# reload This command will reboot the system. (y/n)? [n] y
```

4. Apply the same RCF and save the running configuration for a second time.

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-config echo-commands cs2# copy running-config startup-config [################################# 100% Copy complete
```

- 5. Verify the health of cluster ports on the cluster.
 - a. Verify that e0d ports are up and healthy across all nodes in the cluster: network port show -role cluster

```
Cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore

Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
```

				0000	. /1.0000	
	Cluster	Cluster	up	9000	auto/10000	healthy
false	01	Clarks.		0000		h 1 + h
e0b false	Cluster	Cluster	up	9000	auto/10000	neartny
laise						
Node: clu	ster1-02					
Ignore						
Health					Speed(Mbps)	Health
	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status	-					
e0a	Cluster	Cluster	up	9000	auto/10000	healthv
false			- 1			<u>1</u>
e0b	Cluster	Cluster	up	9000	auto/10000	healthy
false						
Node: clu	ster1-03					
Node: clu Ignore	ster1-03					
Ignore	ster1-03				Speed(Mbps)	Health
Ignore Health						
Ignore Health Port		Broadcast Domain	Link	MTU		
Ignore Health Port		Broadcast Domain	Link	MTU		
Ignore Health Port	IPspace	Broadcast Domain	Link	MTU		
Ignore Health Port Status	IPspace					Status
Ignore Health Port Status e0a	IPspace Cluster				Admin/Oper	Status
Ignore Health Port Status e0a healthy f	IPspace Cluster	Cluster	 up	9000	Admin/Oper	Status
Ignore Health Port Status e0a healthy f	IPspace Cluster alse Cluster	Cluster	 up	9000	Admin/Operauto/100000	Status
Ignore Health Port Status e0a healthy f e0d healthy f	IPspace Cluster alse Cluster alse	Cluster	 up	9000	Admin/Operauto/100000	Status
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu	IPspace Cluster alse Cluster alse	Cluster	 up	9000	Admin/Operauto/100000	Status
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu Ignore	IPspace Cluster alse Cluster alse	Cluster	 up	9000	Admin/Operauto/100000	Status
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu Ignore Health	IPspace Cluster alse Cluster alse ster1-04	Cluster Cluster	up up	9000	Admin/Oper auto/100000 auto/100000 Speed(Mbps)	Status) Health
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu Ignore Health Port	IPspace Cluster alse Cluster alse ster1-04	Cluster	up up	9000	Admin/Oper auto/100000 auto/100000 Speed(Mbps)	Status) Health
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu Ignore Health	IPspace Cluster alse Cluster alse ster1-04	Cluster Cluster	up up	9000	Admin/Oper auto/100000 auto/100000 Speed(Mbps)	Status) Health
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu Ignore Health Port	IPspace Cluster alse Cluster alse ster1-04 IPspace	Cluster Cluster	up up	9000	Admin/Oper auto/100000 auto/100000 Speed(Mbps)	Status) Health
Ignore Health Port Status e0a healthy f e0d healthy f Node: clu Ignore Health Port Status	IPspace Cluster alse Cluster alse ster1-04 IPspace	Cluster Cluster	up up Link	9000 9000 MTU	Admin/Oper auto/100000 auto/100000 Speed(Mbps) Admin/Oper	Status) Health Status

e0d	Cluster	Cluster	up	9000	auto/100000
healthy	false				
8 entri	es were displ	ayed.			

b. Verify the switch health from the cluster (this might not show switch cs2, since LIFs are not homed on e0d).

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				
				-
cluster1-0	_			
	e0a	cs1	Ethernet1/7	N3K-
C3232C				0
	e0d	cs2	Ethernet1/7	N3K-
C3232C	0 /1			
cluster01-	_	ag1	Ethornot1/0	ערכוו
C3232C	e0a	cs1	Ethernet1/8	N3K-
032320	e0d	cs2	Ethernet1/8	N3K-
C3232C	euu	652	PCHETHECT\0	11011
cluster01-	3/cdp			
0_4000101	e0a	cs1	Ethernet1/1/1	N3K-
C3232C	000	331		1.01.
	e0b	cs2	Ethernet1/1/1	N3K-
C3232C				
cluster1-0	4/cdp			
	e0a	cs1	Ethernet1/1/2	N3K-
C3232C				
	e0b	cs2	Ethernet1/1/2	N3K-
C3232C				
	_	em cluster-switch show -is-	-monitoring-enabled	i
-operation	al true			
Switch		Type	Address	Model
cs1		alustor-notyonh	10.233.205.90	изк-
C3232C		Clustel-Herwolk	10.233.203.90	
	l Number	: FOXXXXXXGD		
	onitored			
20 11		n: None		
Software		n: Cisco Nexus Operating Sy	ystem (NX-OS) Softw	ware,
Version				,

CS2 cluster-network 10.233.205.91 N3K-C3232C
Serial Number: FOXXXXXXXGS
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
9.3(4)
Version Source: CDP
2 entries were displayed.

You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch



2020 Nov 17 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on VLAN0092. Port consistency restored. 2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001. Inconsistent peer vlan. 2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092. Inconsistent local vlan.

6. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes.

The following example uses the interface example output from step 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

7. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds. network interface show -role cluster

Cluster	1::">	> network interface			C
Current	Τα	Logical	Status	Network	Current
	_	Interface	Admin/Oper	Address/Mask	Node
Port			Admini/Oper	Addless/Mask	Node
	_				
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	fals	se			
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true	е			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	fals				
0.1		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0d	true	-	/	1.00 054 1 2/02	1 1 00
e0b	fals	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
eub	Idl		up/up	169.254.1.1/23	cluster1-03
e0b	true	-	up/up	109.254.1.1/25	Clustell-03
C0D	CIU	cluster1-04 clus1	מוו/מוו	169.254.1.6/23	cluster1-04
e0b	fals	-	αρ/αρ	103.201.1.0,20	01450011 01
		cluster1-04 clus2	up/up	169.254.1.7/23	cluster1-04
e0b	true	_			
8 entri	es we	ere displayed.			

8. Verify that the cluster is healthy:

cluster show

cluster1::*> cluste	r show		
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were disp	layed.		
cluster1::*>			

- 9. Repeat Steps 7 to 14 on switch cs1.
- 10. Enable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif \* -auto
-revert True
```

11. Reboot switch cs1. You do this to trigger the cluster LIFs to revert to their home ports. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs1# reload This command will reboot the system. (y/n)? [n] y
```

12. Verify that the switch ports connected to the cluster ports are up.

cs1# show	interface	brief	\ grep	up		
•	1	eth	access	up	none	10G(D)
 Eth1/1/2	1	eth	access	up	none	10G(D)
Eth1/7	1	eth	trunk	up	none	100G(D)
Eth1/8	1	eth	trunk	up	none	100G(D)
•						
•						

13. Verify that the ISL between cs1 and cs2 is functional:

show port-channel summary

14. Verify that the cluster LIFs have reverted to their home port:

network interface show -role cluster

		Logical	Status	Network	Current
Current	Is				
Vserver	•	Interface	Admin/Oper	Address/Mask	Node
Port	_	e 			
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	tru				
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	tru		,	1.00 0.7.1 0.0/00	
- 0 -1	4	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	tru	e cluster1-02 clus2	110/110	169.254.3.9/23	cluster1-02
e0d	true	_	up/up	109.234.3.9/23	Clustell-02
00 a	or a	cluster1-03 clus1	up/up	169.254.1.3/23	cluster1-03
e0b	tru	_	-1, -1		
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	tru	e –			
		cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	tru	е			
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0b	tru	e ere displayed.			

15. Verify that the cluster is healthy:

cluster show

<pre>cluster1::*> cluster Node</pre>	show Health	Eligibility	Epsilon
-1			 false
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displ	ayed.		
cluster1::*>			

16. Ping the remote cluster interfaces to verify connectivity: cluster ping-cluster -node local

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03 clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03 clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04 clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04 clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01 clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01 clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02 clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02 clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
. . . . . . . . . . . .
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
   Local 169.254.1.3 to Remote 169.254.1.7
   Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
   Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
   Local 169.254.1.1 to Remote 169.254.3.5
   Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Migrate a CN1610 switch to a Cisco Nexus 3232C cluster switch

You must be aware of certain configuration information, port connections, and cabling requirements when you replace CN1610 cluster switches with Cisco Nexus 3232C cluster switches.

The cluster switches support the following node connections:

- NetApp CN1610: ports 0/1 through 0/12 (10 GbE)
- Cisco Nexus 3232C: ports e1/1-30 (40 or 100 or 4x10GbE)

The cluster switches use the following inter-switch link (ISL) ports.

- NetApp CN1610: ports 0/13 through 0/16 (10 GbE)
- Cisco Nexus 3232C: ports 1/31-32 (100GbE)



You must use 4x10G breakout cables on the Cisco Nexus 3232C cluster switch.

The following table shows the cabling connections that are required at each stage as you make the transition from NetApp CN1610 switches to Cisco Nexus 3232C cluster switches:

Stage	Description	Required cables
Initial	CN1610 to CN1610 (SFP+ to SFP+)	4 SFP+ optical fiber or copper direct-attach cables
Transition	CN1610 to 3232C (QSFP to SFP+)	1 QSFP and 4 SFP+ optical fiber or copper breakout cables
Final	3232C to 3232C (QSFP to QSFP)	2 QSFP optical fiber or copper direct-attach cables

You must have downloaded the applicable reference configuration files (RCFs). The number of 10 GbE and 40/100 GbE ports are defined in the RCFs available on the Cisco® Cluster Network Switch Reference Configuration File Download page.

The ONTAP and NX-OS versions that are supported in this procedure are listed on the Cisco Ethernet Switches page.

The ONTAP and FASTPATH versions that are supported in this procedure are listed on the NetApp CN1601 and CN1610 Switches page.

How to migrate a CN1610 cluster switch to a Cisco Nexus 3232C cluster switch

To replace the existing CN1610 cluster switches in a cluster with Cisco Nexus 3232C cluster switches, you must perform a specific sequence of tasks.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The nodes are n1, n2, n3, and n4.
- The command outputs might vary depending on different releases of ONTAP software.
- The CN1610 switches to be replaced are CL1 and CL2.
- The Nexus 3232C switches to replace the CN1610 switches are C1 and C2.
- n1_clus1 is the first cluster logical interface (LIF) that is connected to cluster switch 1 (CL1 or C1) for node

n1.

- n1 clus2 is the first cluster LIF that is connected to cluster switch 2 (CL2 or C2) for node n1.
- n1_clus3 is the second LIF that is connected to cluster switch 2 (CL2 or C2) for node n1.
- n1 clus4 is the second LIF that is connected to cluster switch 1 (CL1 or C1) for node n1.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.

Procedure summary

The following list describes the stages you must complete when changing the cluster switches:

- I. Replace cluster switch CL2 with C2 (Steps 1-22)
- II. Replace cluster switch CL1 with C1 (Steps 23-40)

The examples in this procedure use four nodes: Two nodes use four 10 GbE cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40 GbE cluster interconnect fiber cables: e4a and e4e. The *Hardware Universe* has information about the cluster fiber cables on your platforms.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

x is the duration of the maintenance window in hours.



The message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Display information about the devices in your configuration: network device-discovery show

The following example displays how many cluster interconnect interfaces have been configured in each node for each cluster interconnect switch:

	Local	Discovered		
Node	Port	Device	Interface	Platform
n1	 /cdp			
	e0a	CL1	0/1	CN1610
	e0b	CL2	0/1	CN1610
	e0c	CL2	0/2	CN1610
	e0d	CL1	0/2	CN1610
n2	/cdp			
	e0a	CL1	0/3	CN1610
	e0b	CL2	0/3	CN1610
	e0c	CL2	0/4	CN1610
	e0d	CL1	0/4	CN1610

- 3. Determine the administrative or operational status for each cluster interface.
 - a. Display the cluster network port attributes: network port show -role cluster

	(network	x port show)					
Node:	n1						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	Health
Status	5						
e0a	cluster	cluster	up	9000	auto/10000	_	
e0b	cluster	cluster	up	9000	auto/10000	_	
e0c	cluster	cluster	up	9000	auto/10000	_	_
e0d	cluster	cluster	up	9000	auto/10000	-	-
Node:	n2						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	Health
Status	5						
e0a	cluster	cluster	up	9000	auto/10000	_	
e0b	cluster	cluster	up	9000	auto/10000	_	
e0c	cluster		up	9000	auto/10000	_	
e0d	cluster	cluster	up	9000	auto/10000	_	

b. Display information about the logical interfaces: network interface show -role cluster

	interface Logical		Network	Current	Current	Is
Vserver	-		Address/Mask	Node	Port	Home
Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2 clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2 clus4	up/up	10.10.0.8/24	n2	e0d	true

C. Display information about the discovered cluster switches: system cluster-switch show

The following example displays the cluster switches that are known to the cluster along with their management IP addresses:

Switch 	Type	Address	Model
 CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 012345	67		
Is Monitored: true			
Reason:			
Software Version: 1.2.0.	7		
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 012345	68		
Is Monitored: true			
Reason:			
Software Version: 1.2.0.	7		
Version Source: ISDP			

4. Verify that the appropriate RCF and image are installed on the new 3232C switches as necessary for your requirements, and make any essential site customizations.

You should prepare both switches at this time. If you need to upgrade the RCF and image, you must

complete the following procedure:

- a. See the Cisco Ethernet Switch page on the NetApp Support Site.
- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of the RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software at Cisco® Cluster and Management Network Switch Reference Configuration File Download.
- 5. Migrate the LIFs associated with the second CN1610 switch that you plan to replace: network interface migrate -verser cluster -lif lif-name -source-node source-node-name destination-node destination-node-name -destination-port destination-port-name

You must migrate each LIF individually as shown in the following example:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver cluster -lif n1_clus3
-source-node n1
-destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver cluster -lif n2_clus2
-source-node n2
-destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver cluster -lif n2_clus3
-source-node n2
-destination-node n2 -destination-port e0d
```

6. Verify the cluster's health: network interface show -role cluster

(interface Logical	Status	Network	Current	Current	Is
Vserver			Address/Mask	Node	Port	Home
 Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0a	false
	n1_clus3	up/up	10.10.0.3/24	n1	e0d	false
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0a	false
	n2_clus3	up/up	10.10.0.7/24	n2	e0d	false
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	true

7. Shut down the cluster interconnect ports that are physically connected to switch CL2:

```
network port modify -node node-name -port port-name -up-admin false
```

The following example shows the four cluster interconnect ports being shut down for node n1 and node n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

8. Ping the remote cluster interfaces, and then perform a remote procedure call server check:

```
cluster ping-cluster -node node-name
```

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                        e0b
                                10.10.0.2
Cluster n1_clus3 n1
                         e0c 10.10.0.3
Cluster n1 clus4 n1
                        e0d
                               10.10.0.4
Cluster n2 clus1 n2
                         e0a
                               10.10.0.5
Cluster n2 clus2 n2
                         e0b
                               10.10.0.6
Cluster n2 clus3 n2
                         e0c
                                10.10.0.7
Cluster n2_clus4 n2
                         e0d
                                10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293 Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

9. Shut down the ISL ports 13 through 16 on the active CN1610 switch CL1 using the appropriate command.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISL ports 13 through 16 being shut down on the CN1610 switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface 0/13-0/16
(CL1) (Interface 0/13-0/16) # shutdown (CL1) (Interface 0/13-0/16) # exit
(CL1) (Config) # exit
(CL1) #
```

10. Build a temporary ISL between CL1 and C2:

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows a temporary ISL being built between CL1 (ports 13-16) and C2 (ports e1/24/1-4) using the Cisco switchport mode trunk command:

```
C2# configure

C2(config)# interface port-channel 2

C2(config-if)# switchport mode trunk

C2(config-if)# spanning-tree port type network

C2(config-if)# mtu 9216

C2(config-if)# interface breakout module 1 port 24 map 10g-4x

C2(config)# interface e1/24/1-4

C2(config-if-range)# switchport mode trunk

C2(config-if-range)# mtu 9216

C2(config-if-range)# channel-group 2 mode active

C2(config-if-range)# exit

C2(config-if)# exit
```

11. Remove the cables that are attached to the CN1610 switch CL2 on all the nodes.

Using supported cabling, you must reconnect the disconnected ports on all the nodes to the Nexus 3232C switch C2.

12. Remove four ISL cables from ports 13 to 16 on the CN1610 switch CL1.

You must attach the appropriate Cisco QSFP28 to SFP+ breakout cables connecting port 1/24 on the new Cisco 3232C switch C2 to ports 13 to 16 on the existing CN1610 switch CL1.



When reconnecting any cables to the new Cisco 3232C switch, the cables used must be either optical fiber or Cisco twinax cables.

13. Make the ISL dynamic by configuring the ISL interface 3/1 on the active CN1610 switch to disable the static mode.

This configuration matches with the ISL configuration on the 3232C switch C2 when the ISLs are brought up on both switches in Step 10.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the ISL interface 3/1 being configured to make the ISL dynamic:

```
(CL1) # configure
(CL1) (Config) # interface 3/1
(CL1) (Interface 3/1) # no port-channel static
(CL1) (Interface 3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

14. Bring up ISLs 13 through 16 on the active CN1610 switch CL1.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISL ports 13 through 16 being brought up on the port-channel interface 3/1:

```
(CL1) # configure
(CL1) (Config) # interface 0/13-0/16,3/1
(CL1) (Interface 0/13-0/16,3/1) # no shutdown
(CL1) (Interface 0/13-0/16,3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

15. Verify that the ISLs are up on the CN1610 switch CL1.

The "Link State" should be Up, "Type" should be Dynamic, and the "Port Active" column should be True for ports 0/13 to 0/16.

The following example shows the ISLs being verified as up on the CN1610 switch CL1:

```
(CL1) # show port-channel 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr
    Device/
             Port
                     Port
Ports Timeout
             Speed
                    Active
0/13 actor/long
            10 Gb Full True
   partner/long
0/14 actor/long
            10 Gb Full True
   partner/long
0/15 actor/long
            10 Gb Full True
    partner/long
0/16
    actor/long 10 Gb Full True
                            partner/long
```

16. Verify that the ISLs are up on the 3232C switch C2: show port-channel summary

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

Ports Eth1/24/1 through Eth1/24/4 should indicate (P), meaning that all four ISL ports are up in the port channel. Eth1/31 and Eth1/32 should indicate (D) as they are not connected.

The following example shows the ISLs being verified as up on the 3232C switch C2:

```
C2# show port-channel summary

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

-----

Group Port Type Protocol Member Ports

Channel

-----

1 Pol(SU) Eth LACP Eth1/31(D) Eth1/32(D)

2 Po2(SU) Eth LACP Eth1/24/1(P) Eth1/24/2(P)

Eth1/24/3(P)
```

17. Bring up all of the cluster interconnect ports that are connected to the 3232C switch C2 on all of the nodes: network port modify -node node-name -port port-name -up-admin true

The following example shows how to bring up the cluster interconnect ports connected to the 3232C switch C2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true cluster::*> network port modify -node n1 -port e0c -up-admin true cluster::*> network port modify -node n2 -port e0b -up-admin true cluster::*> network port modify -node n2 -port e0c -up-admin true
```

18. Revert all of the migrated cluster interconnect LIFs that are connected to C2 on all of the nodes: network interface revert -vserver cluster -lif lif-name

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
```

19. Verify that all of the cluster interconnect ports are reverted to their home ports: network interface show -role cluster

The following example shows that the LIFs on clus2 are reverted to their home ports; the LIFs are successfully reverted if the ports in the "Current Port" column have a status of true in the "Is Home" column. If the "Is Home" value is false, then the LIF is not reverted.

(Hecwork	interface	,				_
	Logical	Status	Network	Current	Current	Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	Home
Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2 clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2 clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2 clus4	up/up	10.10.0.8/24	n2	e0d	true

20. Verify that all of the cluster ports are connected: network port show -role cluster

The following example shows the output verifying all of the cluster interconnects are up:

clust		work port show)	low -ro	le clu	ster		
Node:	n1						
		Broadcast			Speed (Mbps)		Ignore
Port Status	-	Domain	Link	MTU	Admin/Open	Status	Health
							-
e0a	cluster	cluster	up	9000	auto/10000	_	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	_	_
e0d	cluster	cluster	up	9000	auto/10000	_	_
Node:	n2						
		Broadcast			Speed (Mbps)	Health	Ignore
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	Health
Status	3						
							-
e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
	cluster		up	9000	auto/10000	-	
e0d	cluster	cluster	up	9000	auto/10000	-	
8 ent:	ries were	displayed.					

21. Ping the remote cluster interfaces and then perform a remote procedure call server check: cluster ping-cluster -node node-name

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1
                         e0a 10.10.0.1
Cluster n1 clus2 n1
                        e0b
                                10.10.0.2
Cluster n1 clus3 n1
                         e0c 10.10.0.3
                                10.10.0.4
Cluster n1 clus4 n1
                        e0d
Cluster n2 clus1 n2
                         e0a 10.10.0.5
Cluster n2 clus2 n2
                        e0b 10.10.0.6
Cluster n2 clus3 n2
                         e0c
                                10.10.0.7
                          e0d 10.10.0.8
Cluster n2 clus4 n2
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.2 to Remote 10.10.0.5
   Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
   Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

22. Migrate the LIFs that are associated with the first CN1610 switch CL1: network interface migrate -vserver cluster -lif *lif-name* -source-node *node-name*

You must migrate each cluster LIF individually to the appropriate cluster ports hosted on cluster switch C2 as shown in the following example:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1
-source-node n1
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n1_clus4
-source-node n1
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver cluster -lif n2_clus1
-source-node n2
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n2_clus4
-source-node n2
-destination-node n2 -destination-port e0c
```

23. Verify the cluster's status: network interface show -role cluster

The following example shows that the required cluster LIFs have been migrated to the appropriate cluster ports hosted on cluster switch C2:

	Logical	Status	Network	Current	Current	Is
server	Interface	Admin/Oper	Address/Mask	Node	Port	Home
Cluster		,		_		
	n1_clus1	up/up	10.10.0.1/24	n1	e0b	false
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0c	false
	n2 clus1	up/up	10.10.0.5/24	n2	e0b	false
	n2 clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2 clus4	up/up	10.10.0.8/24	n2	e0c	false

24. Shut down the node ports that are connected to CL1 on all of the nodes: network port modify -node node-name -port port-name -up-admin false

The following example shows specific ports being shut down on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

25. Shut down the ISL ports 24, 31, and 32 on the active 3232C switch C2.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISLs 24, 31, and 32 being shut down on the active 3232C switch C2:

```
C2# configure
C2(config)# interface ethernet 1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if-range)# exit
C2(config)# exit
```

26. Remove the cables that are attached to the CN1610 switch CL1 on all of the nodes.

Using the appropriate cabling, you must reconnect the disconnected ports on all the nodes to the Nexus 3232C switch C1.

27. Remove the QSFP28 cables from Nexus 3232C C2 port e1/24.

You must connect ports e1/31 and e1/32 on C1 to ports e1/31 and e1/32 on C2 using supported Cisco QSFP28 optical fiber or direct-attach cables.

28. Restore the configuration on port 24 and remove the temporary port-channel 2 on C2:

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the running-configuration file being copied to the startup-configuration file:

```
C2# configure
C2(config) # no interface breakout module 1 port 24 map 10g-4x
C2(config) # no interface port-channel 2
C2(config-if) # interface e1/24
C2(config-if) # description 100GbE/40GbE Node Port
C2(config-if) # spanning-tree port type edge
Edge port type (portfast) should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when edge port type (portfast) is enabled, can cause temporary
bridging loops.
Use with CAUTION
Edge Port Type (Portfast) has been configured on Ethernet 1/24 but will
only
have effect when the interface is in a non-trunking mode.
C2(config-if) # spanning-tree bpduguard enable
C2(config-if) # mtu 9216
C2(config-if-range) # exit
C2(config)# exit
C2# copy running-config startup-config
[############ 100%
Copy Complete.
```

29. Bring up ISL ports 31 and 32 on C2, the active 3232C switch.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISLs 31 and 32 being brought upon the 3232C switch C2:

30. Verify that the ISL connections are up on the 3232C switch C2.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the ISL connections being verified. Ports Eth1/31 and Eth1/32 indicate (P), meaning that both the ISL ports are up in the port-channel:

```
C1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       S - Switched R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
    Channel
1 Po1(SU) Eth LACP Eth1/31(P) Eth1/32(P)
C2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
      I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       S - Switched R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
_____
Group Port- Type Protocol Member Ports
    Channel
1 Po1(SU) Eth LACP Eth1/31(P) Eth1/32(P)
```

31. Bring up all of the cluster interconnect ports connected to the new 3232C switch C1 on all of the nodes: network port modify -node node-name -port port-name -up-admin true

The following example shows all of the cluster interconnect ports connected to the new 3232C switch C1 being brought up:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

32. Verify the status of the cluster node port: network port show -role cluster

The following example shows output that verifies that the cluster interconnect ports on nodes n1 and n2 on the new 3232C switch C1 are up:

```
cluster::*> network port show -role cluster
     (network port show)
Node: n1
          Broadcast
                           Speed (Mbps) Health Ignore
Port IPspace Domain Link MTU Admin/Open Status Health
Status
_____
e0a cluster cluster up 9000 auto/10000
e0b cluster cluster up 9000 auto/10000 e0c cluster cluster up 9000 auto/10000
e0d cluster cluster up 9000 auto/10000 -
Node: n2
          Broadcast
                            Speed (Mbps) Health Ignore
Port IPspace Domain Link MTU Admin/Open Status Health
Status
_____
e0a cluster cluster up 9000 auto/10000
e0b cluster cluster up 9000 auto/10000
e0c cluster cluster up 9000 auto/10000
e0d cluster cluster up 9000 auto/10000
8 entries were displayed.
```

33. Revert all of the migrated cluster interconnect LIFs that were originally connected to C1 on all of the nodes: network interface revert -server cluster -lif *lif-name*

You must migrate each LIF individually as shown in the following example:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n1_clus4
cluster::*> network interface revert -vserver cluster -lif n2_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus4
```

34. Verify that the interface is now home: network interface show -role cluster

The following example shows the status of cluster interconnect interfaces is up and "Is Home" for nodes n1 and n2:

(Hecwork	interface	,				_
	Logical	Status	Network	Current	Current	Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	Home
Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2 clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2 clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2 clus4	up/up	10.10.0.8/24	n2	e0d	true

35. Ping the remote cluster interfaces and then perform a remote procedure call server check: cluster ping-cluster -node host-name

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                        e0b
                               10.10.0.2
Cluster n1_clus3 n1 e0c 10.10.0.3
Cluster n1 clus4 n1
                        e0d
                               10.10.0.4
Cluster n2 clus1 n2
                        e0a 10.10.0.5
                        e0b 10.10.0.6
Cluster n2 clus2 n2
Cluster n2 clus3 n2
                        e0c
                               10.10.0.7
Cluster n2 clus4 n2 e0d 10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
   Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
3 paths up, 0 paths down (udp check)
```

- 36. Expand the cluster by adding nodes to the Nexus 3232C cluster switches.
- 37. Display the information about the devices in your configuration:

The following examples show nodes n3 and n4 with 40 GbE cluster ports connected to ports e1/7 and e1/8, respectively, on both the Nexus 3232C cluster switches. Both nodes are joined to the cluster. The 40 GbE cluster interconnect ports used are e4a and e4e.

Node Pont	edp eda C e0b C e0c C	2 2 1	Etherne Etherne Etherne Etherne	et1/1/1 et1/1/1	1 N3K- 1 N3K- 2 N3K-	C32320 C32320 C32320	C C	
n1 /c e e e e n2 /c e e e e e e e e e e e e e e e e e e e	cdp 0a C 0b C 0c C 0d C cdp 0a C	1 2 2 1	Etherne Etherne Etherne Etherne	et1/1/1 et1/1/1	1 N3K- 1 N3K- 2 N3K-	C32320 C32320 C32320	C C	
e e e e e e e e e e e e e e e e e e e	e0a C e0b C e0c C e0d C edp e0a C e0b C	2 2 1	Etherne Etherne Etherne	et1/1/1 et1/1/2	1 N3K- 2 N3K-	C32320 C32320	C	
n2 /c	00b C 00c C 00d C cdp 00a C 00b C	2 2 1	Etherne Etherne Etherne	et1/1/1 et1/1/2	1 N3K- 2 N3K-	C32320 C32320	C	
n2 /c e e e e	eOc Cedp eOa Cedp eOa Cedp eOa Cedp eOa Cedp	2 1 1	Etherne Etherne	et1/1/2	2 N3K-	C32320		
n2 /c	e0d C cdp e0a C e0b C e0c C	1	Etherne				C	
n2 /c e e	edp e0a C e0b C	1		et1/1/2	2 N3K-			
e e e	0a C 0b C		E+b			C32320	C	
e	e0b C		E+b					
е	eOc C		ьunerne	et1/1/3	3 N3K-	C32320	C	
		2	Etherne	et1/1/3	3 N3K-	C32320	C	
е	e0d C	2	Etherne	et1/1/4	4 N3K-	C32320	C	
		1	Etherne	et1/1/4	4 N3K-	C32320	C	
n3 /c	cdp							
е	e4a C	1	Etherne	et1/7	N3K-	C32320	C	
е	e4e C	2	Etherne	et1/7	N3K-	C32320	C	
n4 /c	cdp							
е	e4a C	1	Etherne	et1/8	N3K-	C32320	C	
е	e4e C	2	Etherne	et1/8	N3K-	C32320	C	
12 entrie	es were	displayed.						
cluster::	*> net	work port sh	.ow -rol	le clus	ster			
(network	port s	how)						
Node: n1								
		Broadcast		S	Speed (M	bps) I	Health	Ignore
Port IPs	space		Link N		Admin/Op	_	Status	Health
Status					, - 1-			
								_
e0a clu	ster	cluster	up 9	9000 a	auto/100	0.0	_	
	ster		-		auto/100		_	
e0c clu			_		auto/100			

[°] network device-discovery show

[°] network port show -role cluster

[°] network interface show -role cluster

[°] system cluster-switch show

e0d	cluster	cluster	up	9000	auto/10	000	<u>-</u>			
Node:	n2									
.	T.D.	Broadcast	T ' 1	NATTO	Speed (_			Ignor	
Port Status	_	Domain	Link	MTU	Admin/O	pen	Sta	tus	Healt	:h
e0a	cluster	cluster	up	9000	auto/10	000	_			
e0b	cluster	cluster	up	9000	auto/10	000	-			
e0c	cluster	cluster	up	9000	auto/10	000	-			
e0d	cluster	cluster	up	9000	auto/10	000	-		-	
Node:	n3									
		Broadcast			Speed (_			Ignor	
	IPspace	Domain	Link	MTU	Admin/O	pen	Sta ⁻	tus	Healt	h
Statu	S									
	cluster	cluster	un	9000	auto/40	000	_			
	cluster		up		auto/10		_		_	
		0140001	αp	3000	4455, 15					
Node:	n4								_	
D.	TD	Broadcast	T ' 1	NATIONAL	Speed (_			Ignor	
	IPspace	Domain	Link	M.I.O	Admin/O	pen	Sta	tus	Healt	in
Status	5 									
e4a	cluster	cluster	up	9000	auto/40	000	_			
	cluster		_		auto/40		_			
			1		·					
12 ent	tries were	displayed.								
		work interf	ace sh	now -ro	le clust	er				
(netwo	ork interf				,	_		_		
77~ ~	Logica			Networ						S
vserve	er incerr	ace Admin/	oper	Addres	S/Mask	Node		POIL		lome
Cluste	 -r									
O L a D C		s1 up/up		10.10.	0.1/24	n1		e0a	t	rue
	_	s2 up/up				n1		e0b		rue
	_	s3 up/up						e0c		rue
	_	s4 up/up						e0d		rue
	_	s1 up/up						e0a		rue
	_	s2 up/up				n2				rue
	-	s3 up/up				n2		e0c		rue
	_	_								

	n2_clus4	up/up	10.10.0.8/24	n2	e0d	true
	n3_clus1	up/up	10.10.0.9/24	n3	e4a	true
	n3_clus2	up/up	10.10.0.10/2	24 n3	e4e	true
	n4_clus1	up/up	10.10.0.11/2	24 n4	e4a	true
	n4_clus2	up/up	10.10.0.12/2	24 n4	e4e	true
12 entrie	s were dis	played.				
cluster::	> system c	luster-s	witch show			
Switch			Туре	Address	Mod	el
C1			cluster-network	10.10.1.1	03 NX3	232C
Seri	al Number:	FOXOOOO	1 1			
	Monitored:		0 1			
10	Reason:					
Softwar			exus Operating Sy	stem (NX-0	S) Softw	are,
Version			1 2	,	,	•
		7.0(3)I	6(1)			
Versi	on Source:	CDP				
C2			cluster-network	10.10.1.1	04 NX3	232C
	al Number:		02			
Is	Monitored:	true				
	Reason:					
	e Version:	Cisco Ne	exus Operating Sy	vstem (NX-0	S) Softw	are,
Version						
		7.0(3)I	6(1)			
	on Source:	CDP				
CL1			cluster-network	10.10.1.1	01 CN1	610
Comi	al Number:	0102456	7			
	ar Number: Monitored:		I			
15	Reason:					
Cof+***	Reason: e Version:					
	e version: on Source:					
versi	on source:	ISDE				

Serial Number: 01234568
Is Monitored: true

Reason:

Software Version: 1.2.0.7

Version Source: ISDP 4 entries were displayed.

CL2 cluster-network 10.10.1.102 CN1610

38. Remove the replaced CN1610 switches if they are not automatically removed: system cluster-switch delete -device switch-name

You must delete both devices individually as shown in the following example:

```
cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2
```

39. Verify that the proper cluster switches are monitored: system cluster-switch show

The following example shows cluster switches C1 and C2 are being monitored:

```
cluster::> system cluster-switch show
Switch
                           Type
                                            Address
                                                              Model
C1
                           cluster-network 10.10.1.103 NX3232C
     Serial Number: FOX000001
      Is Monitored: true
           Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3)I6(1)
    Version Source: CDP
C2
                           cluster-network 10.10.1.104 NX3232C
     Serial Number: FOX000002
     Is Monitored: true
         Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   7.0(3)16(1)
    Version Source: CDP
2 entries were displayed.
```

40. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

```
system cluster-switch log setup-password
```

system cluster-switch log enable-collection

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

41. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Related information

NetApp CN1601 and CN1610 description page

Cisco Ethernet Switch description page

Hardware Universe

Migrate from a Cisco Nexus 5596 switch to a Cisco Nexus 3232C switch

You must be aware of certain configuration information, port connections and cabling requirements when you are replacing Cisco Nexus 5596 cluster switches with Cisco Nexus 3232C cluster switches.

- The following cluster switches are used as examples in this procedure:
 - Nexus 5596
 - Nexus 3232C
- The cluster switches use the following ports for connections to nodes:
 - Ports e1/1-40 (10 GbE): Nexus 5596
 - · Ports e1/1-30 (10/40/100 GbE): Nexus 3232C
- The cluster switches use the following Inter-Switch Link (ISL) ports:
 - Ports e1/41-48 (10 GbE): Nexus 5596
 - Ports e1/31-32 (40/100 GbE): Nexus 3232C
- The *Hardware Universe* contains information about supported cabling to Nexus 3232C switches:
 - Nodes with 10 GbE cluster connections require QSFP to SFP+ optical fiber breakout cables or QSFP to SFP+ copper breakout cables.
 - Nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28 optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
- The cluster switches use the appropriate ISL cabling:
 - Beginning: Nexus 5596 (SFP+ to SFP+)
 - 8x SFP+ fiber or copper direct-attach cables
 - Interim: Nexus 5596 to Nexus 3232C (QSFP to 4xSFP+ break-out)
 - 1x QSFP to SFP+ fiber break-out or copper break-out cables
 - Final: Nexus 3232C to Nexus 3232C (QSFP28 to QSFP28)
 - 2x QSFP28 fiber or copper direct-attach cables
- On Nexus 3232C switches, you can operate QSFP/QSFP28 ports in either 40/100 Gigabit Ethernet or 4 x10 Gigabit Ethernet modes.

By default, there are 32 ports in the 40/100 Gigabit Ethernet mode. These 40 Gigabit Ethernet ports are numbered in a 2-tuple naming convention. For example, the second 40 Gigabit Ethernet port is numbered as 1/2. The process of changing the configuration from 40 Gigabit Ethernet to 10 Gigabit Ethernet is called *breakout* and the process of changing the configuration from 10 Gigabit Ethernet to 40 Gigabit Ethernet is called *breakin*. When you break out a 40/100 Gigabit Ethernet port into 10 Gigabit Ethernet ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the break-out ports of the second 40/100 Gigabit Ethernet port are numbered as 1/2/1, 1/2/2, 1/2/3, and 1/2/4.

- On the left side of Nexus 3232C switches are 2 SFP+ ports, called 1/33 and 1/34.
- You have configured some of the ports on Nexus 3232C switches to run at 10 GbE or 40/100 GbE.



You can break out the first six ports into 4x10 GbE mode by using the <code>interface</code> breakout module 1 port 1-6 map 10g-4x command. Similarly, you can regroup the first six QSFP+ ports from breakout configuration by using the no <code>interface</code> breakout module 1 port 1-6 map 10g-4x command.

- You have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3232C cluster switches.
- The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page.

How to migrate from a Cisco Nexus 5596 cluster switch to a Cisco Nexus 3232C cluster switch

To replace existing Cisco Nexus 5596 cluster switches in a cluster with Nexus 3232C cluster switches, you must perform a specific sequence of tasks.

About this task

The examples in this procedure describe replacing Cisco Nexus 5596 switches with Cisco Nexus 3232C switches. You can use these steps (with modifications) for other older Cisco switches (for example, 3132Q-V). The procedure also uses the following switch and node nomenclature:

- The command outputs might vary depending on different releases of ONTAP.
- The Nexus 5596 switches to be replaced are CL1 and CL2.
- The Nexus 3232C switches to replace the Nexus 5596 switches are C1 and C2.
- n1 clus1 is the first cluster logical interface (LIF) connected to cluster switch 1 (CL1 or C1) for node n1.
- n1_clus2 is the first cluster LIF connected to cluster switch 2 (CL2 or C2) for node n1.
- n1 clus3 is the second LIF connected to cluster switch 2 (CL2 or C2) for node n1.
- n1 clus4 is the second LIF connected to cluster switch 1 (CL1 or C1) for node n1.-
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.
- The nodes are n1, n2, n3, and n4.



The examples in this procedure use four nodes: Two nodes use four 10 GbE cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40 GbE cluster interconnect ports: e4a, e4e. The *Hardware Universe* lists the actual cluster ports on your platforms.

This procedure covers the following scenarios:

- The cluster starts with two nodes connected and functioning in a two Nexus 5596 cluster switches.
- The cluster switch CL2 to be replaced by C2 (steps 1 to 19):
 - Traffic on all cluster ports and LIFs on all nodes connected to CL2 are migrated onto the first cluster ports and LIFs connected to CL1.
 - Disconnect cabling from all cluster ports on all nodes connected to CL2, and then use supported breakout cabling to reconnect the ports to new cluster switch C2.
 - Disconnect cabling between ISL ports between CL1 and CL2, and then use supported break-out cabling to reconnect the ports from CL1 to C2.

- Traffic on all cluster ports and LIFs connected to C2 on all nodes is reverted.
- The cluster switch CL2 to be replaced by C2 (steps 20 to 33)
 - Traffic on all cluster ports or LIFs on all nodes connected to CL1 are migrated onto the second cluster ports or LIFs connected to C2.
 - Disconnect cabling from all cluster port on all nodes connected to CL1 and reconnect, using supported break-out cabling, to new cluster switch C1.
 - Disconnect cabling between ISL ports between CL1 and C2, and reconnect using supported cabling, from C1 to C2.
 - Traffic on all cluster ports or LIFs connected to C1 on all nodes is reverted.
- Two FAS9000 nodes have been added to cluster with examples showing cluster details (steps 34 to 37).



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Display information about the devices in your configuration:

```
network device-discovery show
```

The following example shows how many cluster interconnect interfaces have been configured in each node for each cluster interconnect switch:

cluster::>		device-discovery sl Discovered	low	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e0a	CL1	Ethernet1/1	N5K-C5596UP
	e0b	CL2	Ethernet1/1	N5K-C5596UP
	e0c	CL2	Ethernet1/2	N5K-C5596UP
	e0d	CL1	Ethernet1/2	N5K-C5596UP
n2	/cdp			
	e0a	CL1	Ethernet1/3	N5K-C5596UP
	e0b	CL2	Ethernet1/3	N5K-C5596UP
	e0c	CL2	Ethernet1/4	N5K-C5596UP
	e0d	CL1	Ethernet1/4	N5K-C5596UP
8 entries v	were disp	played.		

- 3. Determine the administrative or operational status for each cluster interface:
 - a. Display the network port attributes:

```
network port show -role cluster
```

The following example displays the network port attributes on nodes n1 and n2:

	*> network po k port show)	rt show -role clu	ıster			
Ignore					Speed (Mbpg)	Hoal+b
Health					Speed (Mbps)	неатип
Port Status	IPspace	Broadcast Domair	l Link	MTU	Admin/Oper	Status
e0a -	Cluster	Cluster	up	9000	auto/10000	-
e0b -	Cluster	Cluster	up	9000	auto/10000	-
e0c	Cluster	Cluster	up	9000	auto/10000	-
e0d -	Cluster	Cluster	up	9000	auto/10000	-
Node: n2						
Ignore					Speed(Mbps)	Health
Health	I Dama a a	Decederat Demois	. T 1-	MITT		
Status	Irspace	Broadcast Domair	I LIIK	MTO	Admin/Oper	Status
e0a -	Cluster	Cluster	up	9000	auto/10000	_
e0b	Cluster	Cluster	up	9000	auto/10000	-
e0c	Cluster	Cluster	up	9000	auto/10000	-
e0d -	Cluster	Cluster	up	9000	auto/10000	_
8 entries	were display	ed.				

b. Display information about the logical interfaces:

network interface show -role cluster

The following example displays the general information about all of the LIFs on the cluster, including their current ports:

		nterface sho			
~ .	_	Logical	Status	Network	Current
Current	_	T., + 6	7) -1	7 -1-1	NT1 -
			Admin/Oper	Address/Mask	Noae
Port	HOM	e			
		_			
Cluster		_			
CIUSCCI		n1 clus1	מנו/מנו	10.10.0.1/24	n1
e0a	tru	_	ω _Γ , ω _Γ		
			up/up	10.10.0.2/24	n1
e0b	tru	_			
		n1_clus3	up/up	10.10.0.3/24	n1
e0c	tru	е			
		n1_clus4	up/up	10.10.0.4/24	n1
e0d	tru	е			
		n2_clus1	up/up	10.10.0.5/24	n2
e0a	tru				
		n2_clus2	up/up	10.10.0.6/24	n2
e0b	tru				
		_	up/up	10.10.0.7/24	n2
e0c	tru		,	10 10 0 0 0	
		n2_clus4	up/up	10.10.0.8/24	n2

c. Display information about the discovered cluster switches:

system cluster-switch show

The following example shows the active cluster switches:

```
cluster::*> system cluster-switch show
Switch
                              Type
                                                 Address
Model
CL1
                              cluster-network 10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
                             cluster-network 10.10.1.102
CL2
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
2 entries were displayed.
```

4. Verify that the appropriate RCF and image are installed on the new 3232C switches as necessary for your requirements, and make the essential site customizations, such as users and passwords, network addresses, and other customizations.



You must prepare both switches at this time.

If you need to upgrade the RCF and image, you must complete the following steps:

a. Go to the Cisco Ethernet Switches page on the NetApp Support Site.

Cisco Ethernet Switches

- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of the RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software.

See the ONTAP 8.x or later Cluster and Management Network Switch Reference Configuration Files Download page, and then click the appropriate version.

To find the correct version, see the ONTAP 8.x or later Cluster Network Switch Download page.

5. Migrate the LIFs associated with the second Nexus 5596 switch to be replaced:

```
network interface migrate -vserver Cluster -lif lif-name -source-node source-node-name - destination-node node-name -destination-port destination-port-name
```

The following example shows the LIFs being migrated for nodes n1 and n2; LIF migration must be done on all of the nodes:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

6. Verify the cluster's health:

```
network interface show -role cluster
```

The following example shows the current status of each cluster:

	network in		w -role cluster		
`		Status	Network	Current	
Current Is					
	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true					
	n1_clus2	up/up	10.10.0.2/24	n1	e0a
false	n1 clus3	up/up	10.10.0.3/24	n1	e0d
false	_				
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true		,	10 10 0 7 /01		
true	n2_clus1	up/up	10.10.0.5/24	n2	e0a
crue	n2 clus2	up/up	10.10.0.6/24	n2	e0a
false		1, 1	,		
	n2_clus3	up/up	10.10.0.7/24	n2	e0d
false					
	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true		ما			
8 entries we	ere display	ea.			

7. Shut down the cluster interconnect ports that are physically connected to switch CL2:

```
network port modify -node node-name -port port-name -up-admin false
```

The following commands shut down the specified ports on n1 and n2, but the ports must be shut down on all nodes:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

8. Ping the remote cluster interfaces and perform an RPC server check:

```
cluster ping-cluster -node node-name
```

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                     e0b 10.10.0.2
Cluster n1 clus4 n1
                     e0d 10.10.0.4
Cluster n2 clus3 n2
                     e0c 10.10.0.7
Cluster n2_clus4 n2 e0d 10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
   Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
   Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.2 to Remote 10.10.0.5
   Local 10.10.0.2 to Remote 10.10.0.6
   Local 10.10.0.2 to Remote 10.10.0.7
   Local 10.10.0.2 to Remote 10.10.0.8
   Local 10.10.0.3 to Remote 10.10.0.5
   Local 10.10.0.3 to Remote 10.10.0.6
   Local 10.10.0.3 to Remote 10.10.0.7
   Local 10.10.0.3 to Remote 10.10.0.8
   Local 10.10.0.4 to Remote 10.10.0.5
   Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check
```

9. Shut down ISLs 41 through 48 on CL1, the active Nexus 5596 switch using the Cisco shutdown command.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISLs 41 through 48 being shut down on the Nexus 5596 switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface e1/41-48
(CL1) (config-if-range) # shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

10. Build a temporary ISL between CL1 and C2 using the appropriate Cisco commands.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows a temporary ISL being set up between CL1 and C2:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

11. On all nodes, remove all cables attached to the Nexus 5596 switch CL2.

With supported cabling, reconnect disconnected ports on all nodes to the Nexus 3232C switch C2.

12. Remove all the cables from the Nexus 5596 switch CL2.

Attach the appropriate Cisco QSFP to SFP+ break-out cables connecting port 1/24 on the new Cisco 3232C switch, C2, to ports 45 to 48 on existing Nexus 5596, CL1.

13. Bring up ISLs ports 45 through 48 on the active Nexus 5596 switch CL1.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISLs ports 45 through 48 being brought up:

```
(CL1) # configure
(CL1) (Config) # interface e1/45-48
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

14. Verify that the ISLs are up on the Nexus 5596 switch CL1.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows Ports eth1/45 through eth1/48 indicating (P), meaning that the ISL ports are up in the port-channel.

- 15. Verify that interfaces eth1/45-48 already have `channel-group 1 mode active`in their running configuration.
- 16. On all nodes, bring up all the cluster interconnect ports connected to the 3232C switch C2:

```
network port modify -node node-name -port port-name -up-admin true
```

The following example shows the specified ports being brought up on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

17. On all nodes, revert all of the migrated cluster interconnect LIFs connected to C2:

```
network interface revert -vserver Cluster -lif lif-name
```

The following example shows the migrated cluster LIFs being reverted to their home ports:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

18. Verify all the cluster interconnect ports are now reverted to their home:

```
network interface show -role cluster
```

The following example shows that the LIFs on clus2 reverted to their home ports and shows that the LIFs are successfully reverted if the ports in the Current Port column have a status of true in the Is Home column. If the Is Home value is false, the LIF has not been reverted.

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
	· -				
Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true	n1 clus?	up/up	10.10.0.2/24	n1	e0b
true	III_CIUSZ	ир/ ир	10.10.0.2/24	111	dos
	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true	1 7 4	1	10 10 0 4/04	1	0.1
true	n1_clus4	up/up	10.10.0.4/24	n1	e0d
0140	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true					
true	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true	n2 clus3	up/up	10.10.0.7/24	n2	e0c
true	_	1 . 1	·		
	n2_clus4	up/up	10.10.0.8/24	n2	e0d

19. Verify that the clustered ports are connected:

```
network port show -role cluster
```

The following example shows the result of the previous network port modify command, verifying that all the cluster interconnects are up:

```
cluster::*> network port show -role cluster
 (network port show)
Node: n1
Ignore
                                         Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster
                                     9000 auto/10000 -
                   Cluster
                                 up
e0b
                                up 9000 auto/10000 -
       Cluster
                  Cluster
      Cluster Cluster
                                up 9000 auto/10000 -
e0c
                                up 9000 auto/10000 -
e0d Cluster Cluster
Node: n2
Ignore
                                          Speed (Mbps) Health
Health
Port
       IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
_____
                                     9000 auto/10000 -
e0a Cluster Cluster
                                up
       Cluster Cluster
Cluster Cluster
                                up 9000 auto/10000 -
e0b
      Cluster
                                up 9000 auto/10000 -
e0c
e0d Cluster Cluster
                               up 9000 auto/10000 -
8 entries were displayed.
```

20. Ping the remote cluster interfaces and perform an RPC server check:

```
cluster ping-cluster -node node-name
```

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                      e0b 10.10.0.2
Cluster n1_clus3 n1 e0c 10.10.0.3
Cluster n1 clus4 n1
                     e0d 10.10.0.4
Cluster n2 clus3 n2
                      e0c 10.10.0.7
Cluster n2_clus4 n2 e0d 10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

21. On each node in the cluster, migrate the interfaces associated with the first Nexus 5596 switch, CL1, to be replaced:

network interface migrate -vserver Cluster -lif lif-name -source-node sourcenode-name - destination-node destination-node-name -destination-port destination-port-name

The following example shows the ports or LIFs being migrated on nodes n1 and n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

22. Verify the cluster's status:

network interface show

The following example shows that the required cluster LIFs have been migrated to appropriate cluster ports hosted on cluster switch, C2:

	Logical	Status	Network	Current	
Current Is Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
	_				
Cluster	n1_clus1	up/up	10.10.0.1/24	n1	e0b
false	n1_clus2	up/up	10.10.0.2/24	n1	e0b
crue	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true	n1_clus4	up/up	10.10.0.4/24	n1	e0c
false	n2_clus1	up/up	10.10.0.5/24	n2	e0b
false	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true	n2_clus4	up/up	10.10.0.8/24	n2	e0c
<pre>false 8 entries w</pre>	oro dianlass	od			

23. On all the nodes, shut down the node ports that are connected to CL1:

```
network port modify -node node-name -port port-name -up-admin false
```

The following example shows the specified ports being shut down on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

24. Shut down ISL 24, 31 and 32 on the active 3232C switch C2.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ISLs being shutdown:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if-range)# exit
C2(config-if)# exit
```

25. On all nodes, remove all cables attached to the Nexus 5596 switch CL1.

With supported cabling, reconnect disconnected ports on all nodes to the Nexus 3232C switch C1.

26. Remove the QSFP breakout cable from Nexus 3232C C2 ports e1/24.

Connect ports e1/31 and e1/32 on C1 to ports e1/31 and e1/32 on C2 using supported Cisco QSFP optical fiber or direct-attach cables.

27. Restore the configuration on port 24 and remove the temporary Port Channel 2 on C2.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the configuration on port m24 being restored using the appropriate Cisco commands:

28. Bring up ISL ports 31 and 32 on C2, the active 3232C switch, by entering the following Cisco command: no shutdown

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the Cisco commands switchname configure brought up on the 3232C switch C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
```

29. Verify that the ISL connections are up on the 3232C switch C2.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

Ports eth1/31 and eth1/32 should indicate (P) meaning that both ISL ports up in the port-channel

```
C1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

------
Group Port- Type Protocol Member Ports
Channel
-------
1 Pol(SU) Eth LACP Eth1/31(P) Eth1/32(P)
```

30. On all nodes, bring up all the cluster interconnect ports connected to the new 3232C switch C1: network port modify

The following example shows all the cluster interconnect ports being brought up for n1 and n2 on the 3232C switch C1:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

31. Verify the status of the cluster node port:

```
network port show
```

The following example shows verifies that all cluster interconnect ports on all nodes on the new 3232C switch C1 are up:

```
cluster::*> network port show -role cluster
 (network port show)
Node: n1
Ignore
                                        Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster
                              up 9000 auto/10000 -
                 Cluster
e0b
      Cluster Cluster
                              up 9000 auto/10000 -
      Cluster
                              up 9000 auto/10000 -
e0c
                 Cluster
e0d Cluster Cluster up 9000 auto/10000 -
Node: n2
Ignore
                                        Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster
                 Cluster
                              up 9000 auto/10000 -
      Cluster Cluster
                              up 9000 auto/10000 -
e0b
                              up 9000 auto/10000 -
e0c
      Cluster
                 Cluster
e0d Cluster Cluster up 9000 auto/10000 -
8 entries were displayed.
```

32. On all nodes, revert the specific cluster LIFs to their home ports:

```
network interface revert -server Cluster -lif lif-name
```

The following example shows the specific cluster LIFs being reverted to their home ports on nodes n1 and n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

33. Verify that the interface is home:

network interface show -role cluster

The following example shows the status of cluster interconnect interfaces are up and Is Home for n1 and n2:

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>							
	Logical	Status	Network	Current			
Current Is							
	Interface	Admin/Oper	Address/Mask	Node	Port		
Home							
Cluster							
0140001	n1 clus1	up/up	10.10.0.1/24	n1	e0a		
true	_						
	n1_clus2	up/up	10.10.0.2/24	n1	e0b		
true							
	n1_clus3	up/up	10.10.0.3/24	n1	e0c		
true	n1 clus4	/n	10.10.0.4/24	n1	e0d		
true	III_CIUS4	ир/ ир	10.10.0.4/24	111	eua		
cruc	n2 clus1	up/up	10.10.0.5/24	n2	e0a		
true	_						
	n2_clus2	up/up	10.10.0.6/24	n2	e0b		
true							
	n2_clus3	up/up	10.10.0.7/24	n2	e0c		
true	0 1 4		10 10 0 0/04	0	- 0 -1		
true	nz_clus4	up/up	10.10.0.8/24	n2	e0d		
8 entries we	ara dianlass	a d					

34. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster -node node-name

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1 clus1 n1 e0a 10.10.0.1
Cluster n1 clus2 n1
                      e0b 10.10.0.2
Cluster n1_clus3 n1 e0c 10.10.0.3
Cluster n1 clus4 n1
                      e0d 10.10.0.4
Cluster n2 clus3 n2
                      e0c 10.10.0.7
Cluster n2 clus4 n2 e0d 10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

35. Expand the cluster by adding nodes to the Nexus 3232C cluster switches.

The following examples show nodes n3 and n4 have 40 GbE cluster ports connected to ports e1/7 and e1/8 respectively on both the Nexus 3232C cluster switches, and both nodes have joined the cluster. The

40 GbE cluster interconnect ports used are e4a and e4e.

36. Display the information about the devices in your configuration:

[°] system cluster-switch show

		<pre>device-discovery Discovered</pre>		
Node	Port	Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C
12 entries	were di	splayed.		

[°] network device-discovery show

[°] network port show -role cluster

[°] network interface show -role cluster

e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d	Cluster	Cluster		up	9000	auto/10000	-
Node: n2							
Ignore							
_						Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a -	Cluster	Cluster		up	9000	auto/10000	-
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d -	Cluster	Cluster		up	9000	auto/10000	-
Node: n3							
_							
Ignore						Speed (Mbps)	Health
Health							
Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e4a	Cluster	Cluster		up	9000	auto/40000	-
e4e	Cluster	Cluster		up	9000	auto/40000	-
Node: n4							
Ignore						Speed(Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
1010							

Status						
e4a	Cluster	Cluster	up	9000	auto/40000	-
e4e -	Cluster	Cluster	up	9000	auto/40000	_

12 entries were displayed.

	Logical	Status	Network	Current
Current 		- 1 / 6	- 11 / 1	
Vserver Port		ce Admin/Ope	er Address/Mask	Node
Cluster				
	_	l up/up	10.10.0.1/24	n1
e0a		2/	10 10 0 2/24	n 1
e0b	_	z up/up	10.10.0.2/24	n1
COD		מנו/מנו	10.10.0.3/24	n1
e0c	_	ар, ар	10.10.000	
	n1_clus	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus	l up/up	10.10.0.5/24	n2
e0a	true			
0.1	_	2 up/up	10.10.0.6/24	n2
e0b	true	2 110/110	10 10 0 7/24	n2
e0c	true	5 up/up	10.10.0.7/24	112
000		up/up	10.10.0.8/24	n2
e0d	_	1 . 1	,	
	n3_clus	l up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	2 up/up	10.10.0.10/24	n3
e4e	true			
4	_	l up/up	10.10.0.11/24	n4
e4a	true	2 110/110	10 10 0 10/04	n 1
e4e	n4_clus2	2 up/up	10.10.0.12/24	n4

cluster::*> system cluster-switch show Switch Type Address Model cluster-network 10.10.1.103 NX3232C C1Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I4(1)Version Source: CDP C2 cluster-network 10.10.1.104 NX3232C Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP CL1 cluster-network 10.10.1.101 NX5596 Serial Number: 01234567 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.1(1)N1(1) Version Source: CDP CL2 cluster-network 10.10.1.102 NX5596 Serial Number: 01234568 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.1(1)N1(1) Version Source: CDP 4 entries were displayed.

37. Remove the replaced Nexus 5596 by using the system cluster-switch delete command, if it is not automatically removed: system cluster-switch delete -device switch-name

cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2

38. Verify that the proper cluster switches are monitored: system cluster-switch show

cluster::> system cluster-switch show Switch Address Model Type C1 cluster-network 10.10.1.103 NX3232C Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3) I4(1) Version Source: CDP C2 cluster-network 10.10.1.104 NX3232C Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I4(1)Version Source: CDP 2 entries were displayed.

39. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

system cluster-switch log setup-password
system cluster-switch log enable-collection

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

40. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

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

Related information

Cisco Ethernet Switch description page

Hardware Universe

Migrate from a two-node switchless cluster to a cluster with Cisco Nexus 3232C cluster switches

You must be aware of certain configuration information, port connections, and cabling requirements when you migrate a two-node switchless cluster to a cluster with Cisco Nexus 3232C cluster switches.

The Cisco Ethernet Switches page has information about the ONTAP and NX-OS versions supported in this procedure.

You must have the following before you begin the migration process:

· Available ports for node connections

The cluster switches use the Inter-Switch Link (ISL) ports e1/31-32.

-

- · Appropriate cables for cluster connections:
 - The nodes with 10 GbE cluster connections require QSFP optical modules with breakout fiber cables or QSFP to SFP+ copper breakout cables.
 - The nodes with 40/100 GbE cluster connections require supportedQSFP/ QSFP28 optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
 - The cluster switches require the appropriate ISL cabling: 2x QSFP28 fiber or copper direct-attach cables.



See the *Hardware Universe* for further information on cabling systems with Nexus 3232C switches.

How to migrate from a two-node switchless cluster to a cluster with Cisco Nexus 3232C cluster switches

If you have a two-node switchless cluster, you can migrate nondisruptively to a two-node switched cluster that includes Cisco Nexus 3232C cluster network switches.

Before you begin

• The configurations must be properly set up and functioning.

The two nodes must be connected and functioning in a two-node switchless cluster setting.

- All cluster ports must be in the up state.
- Th- Cisco Nexus 3232C cluster switch must be supported.
- The existing cluster network configuration must have the following:
 - A redundant and fully functional Nexus 3232C cluster infrastructure on both switches
 - The latest RCF and NX-OS versions on your switches
 - Management connectivity on both switches
 - · Console access to both switches

- · All cluster logical interfaces (LIFs) in the up state without having been migrated
- Initial customization of the switch
- All ISL ports enabled and cabled

About this task

Procedure summary

- I. Display and migrate physical and logical ports (Steps 1-10)
- II. Shut down the reassigned LIFs and disconnect the cables (Steps 11-14))
- III. Enable the cluster ports (Steps 15-20)
- IV. Enable the reassigned LIFs (Steps 21-33)

The examples in this procedure use the following switch and node nomenclature:

- Nexus 3232C cluster switches, C1 and C2.
- The nodes are n1 and n2.



The examples in this procedure use two nodes, each utilizing two 40 GbE cluster interconnect ports e4a and e4e. The *Hardware Universe* has details about the cluster ports on your platforms.

- n1 clus1 is the first cluster logical interface (LIF) to be connected to cluster switch C1 for node n1.
- n1 clus2 is the first cluster LIF to be connected to cluster switch C2 for node n1.
- n2 clus1 is the first cluster LIF to be connected to cluster switch C1 for node n2.
- n2 clus2 is the second cluster LIF to be connected to cluster switch C2 for node n2.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

- 2. Determine the administrative or operational status for each cluster interface:
 - a. Display the network port attributes:

```
network port show -role cluster
```

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1
Ignore
                                        Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
Node: n2
Ignore
                                        Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
_____ ____
-----
e4a Cluster Cluster up 9000 auto/40000 - e4e Cluster up 9000 auto/40000 -
4 entries were displayed.
```

b. Display information about the logical interfaces and their designated home nodes:

network interface show -role cluster

```
cluster::*> network interface show -role cluster
 (network interface show)
          Logical Status Network
                                               Current
Current Is
          Interface Admin/Oper Address/Mask
Vserver
                                               Node
Port
      Home
Cluster
          n1 clus1 up/up 10.10.0.1/24
                                               n1
e4a
      true
                    up/up 10.10.0.2/24
          n1 clus2
                                               n1
e4e
       true
          n2 clus1
                    up/up
                             10.10.0.3/24
                                               n2
e4a
       true
                    up/up
                             10.10.0.4/24
          n2 clus2
                                               n2
e4e
       true
4 entries were displayed.
```

c. Verify that switchless cluster detection is enabled using the advanced privilege command:

```
network options detect-switchless-cluster show`
```

The output in the following example shows that switchless cluster detection is enabled:

```
cluster::*> network options detect-switchless-cluster show
Enable Switchless Cluster Detection: true
```

3. Verify that the appropriate RCFs and image are installed on the new 3232C switches and make any necessary site customizations such as adding users, passwords, and network addresses.

You must prepare both switches at this time. If you need to upgrade the RCF and image software, you must follow these steps:

a. Go to the Cisco Ethernet Switches page on the NetApp Support Site.

Cisco Ethernet Switches

- b. Note your switch and the required software versions in the table on that page.
- c. Download the appropriate version of RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
- e. Download the appropriate version of the image software.

Cisco Cluster and Management Network Switch Reference Configuration File download page

- Click CONTINUE on the Description page, accept the license agreement, and then follow the instructions
 on the Download page to download the RCF.
- 5. On Nexus 3232C switches C1 and C2, disable all node-facing ports C1 and C2, but do not disable the ISL ports e1/31-32.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ports 1 through 30 being disabled on Nexus 3232C cluster switches C1 and C2 using a configuration supported in RCF NX3232 RCF v1.0 24p10g 24p100g.txt:

```
C1# copy running-config startup-config
[############################### 100% Copy complete.
C1# configure
C1(config) # int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4.e1/7-30
C1(config-if-range) # shutdown
C1(config-if-range) # exit
C1(config)# exit
C2# copy running-config startup-config
[############################### 100% Copy complete.
C2# configure
C2 (config) # int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range) # shutdown
C2(config-if-range) # exit
C2(config)# exit
```

- 6. Connect ports 1/31 and 1/32 on C1 to the same ports on C2 using supported cabling.
- 7. Verify that the ISL ports are operational on C1 and C2:

```
show port-channel summary
```

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the Cisco show port-channel summary command being used to verify the ISL ports are operational on C1 and C2:

```
C1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
      I - Individual H - Hot-standby (LACP only) s - Suspended
r - Module-removed
      S - Switched R - Routed
      U - Up (port-channel)
     M - Not in use. Min-links not met
    Port-
Group Channel Type Protocol Member Ports
1 Po1(SU) Eth LACP Eth1/31(P) Eth1/32(P)
C2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
      I - Individual H - Hot-standby (LACP only) s - Suspended
r - Module-removed
     S - Switched R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
    Po1(SU) Eth LACP Eth1/31(P) Eth1/32(P)
```

8. Display the list of neighboring devices on the switch.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the Cisco command show cdp neighbors being used to display the neighboring devices on the switch:

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                                Port
ΙD
C2
                  Eth1/31
                                174
                                      RSIs
                                                  N3K-C3232C Eth1/31
C2
                  Eth1/32
                                174
                                       RSIs
                                                  N3K-C3232C Eth1/32
Total entries displayed: 2
C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                               Port
ID
C1
                  Eth1/31
                                178
                                       RSIs
                                                  N3K-C3232C Eth1/31
                                                   N3K-C3232C Eth1/32
                  Eth1/32
                                       RSIs
C1
                                178
Total entries displayed: 2
```

9. Display the cluster port connectivity on each node:

network device-discovery show

The following example shows the cluster port connectivity displayed for a two-node switchless cluster configuration:

cluster::*> network device-discovery show Local Discovered							
Modo			Intonfoco	Dlatform			
Node	Port	Device	Interface	Platform			
n1	 /cdp						
	e4a	n2	e4a	FAS9000			
	e4e	n2	e4e	FAS9000			
n2	/cdp						
	e4a	n1	e4a	FAS9000			
	e4e	n1	e4e	FAS9000			

10. Migrate the n1 clus1 and n2 clus1 LIFs to the physical ports of their destination nodes:

network interface migrate -vserver cluster -lif lif-name source-node source-node-name -destination-port destination-port-name

You must execute the command for each local node as shown in the following example:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1
-source-node n1
-destination-node n1 -destination-port e4e
cluster::*> network interface migrate -vserver cluster -lif n2_clus1
-source-node n2
-destination-node n2 -destination-port e4e
```

11. Verify the cluster interfaces have successfully migrated:

```
network interface show -role cluster
```

The following example shows the "Is Home" status for the n1_clus1 and n2_clus1 LIFs has become "false" after the migration is completed:

cluster::*>	network in	terface sho	w -role cluster		
(network i	nterface sh	ow)			
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
	_				
Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e4e
false					
	n1 clus2	up/up	10.10.0.2/24	n1	e4e
true	_				
	n2 clus1	up/up	10.10.0.3/24	n2	e4e
false	_				
	n2 clus2	up/up	10.10.0.4/24	n2	e4e
true	_				
4 entries v	were displa	yed.			

12. Shut down cluster ports for the n1_clus1 and n2_clus1 LIFs, which were migrated in step 9:

```
network port modify -node node-name -port port-name -up-admin false
```

You must execute the command for each port as shown in the following example:

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

13. Ping the remote cluster interfaces and perform an RPC server check:

```
cluster ping-cluster -node node-name
```

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1 clus1 n1
                       e4a 10.10.0.1
Cluster n1 clus2 n1
                          e4e 10.10.0.2
Cluster n2 clus1 n2
                        e4a 10.10.0.3
Cluster n2 clus2 n2 e4e 10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293 Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s) ......
Detected 9000 byte MTU on 32 path(s):
   Local 10.10.0.1 to Remote 10.10.0.3
   Local 10.10.0.1 to Remote 10.10.0.4
   Local 10.10.0.2 to Remote 10.10.0.3
   Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

14. Disconnect the cable from e4a on node n1.

You can refer to the running configuration and connect the first 40 GbE port on the switch C1 (port 1/7 in this example) to e4a on n1 using cabling supported for Nexus 3232C switches.

15. Disconnect the cable from e4a on node n2.

You can refer to the running configuration and connect e4a to the next available 40 GbE port on C1, port 1/8, using supported cabling.

16. Enable all node-facing ports on C1.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows ports 1 through 30 being enabled on Nexus 3232C cluster switches C1 and C2 using the configuration supported in RCF NX3232 RCF v1.0 24p10g 26p100g.txt:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

17. Enable the first cluster port, e4a, on each node:

network port modify -node node-name -port port-name -up-admin true

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

18. Verify that the clusters are up on both nodes:

network port show -role cluster

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
Node: n2
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e4a Cluster Cluster up 9000 auto/40000 - e4e Cluster up 9000 auto/40000 -
e4e
4 entries were displayed.
```

19. For each node, revert all of the migrated cluster interconnect LIFs:

```
network interface revert -vserver cluster -lif lif-name
```

You must revert each LIF to its home port individually as shown in the following example:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus1
```

20. Verify that all the LIFs are now reverted to their home ports:

```
network interface show -role cluster
```

The Is Home column should display a value of true for all of the ports listed in the Current Port column. If the displayed value is false, the port has not been reverted.

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>							
·		Status	Network	Current			
Current Is							
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port		
Home							
	_						
Cluster		,					
	n1_clus1	up/up	10.10.0.1/24	n1	e4a		
true	m1 m1n0		10 10 0 2/24	n1	- 1 -		
true	n1_clus2	up/up	10.10.0.2/24	ΠT	e4e		
crue	n2 clus1	ווח/ווח	10.10.0.3/24	n2	e4a		
true	112_01451	αργαρ	10.10.0.3/21	112	CIG		
0100	n2 clus2	up/up	10.10.0.4/24	n2	e4e		
true	_	1					
4 entries w	ere display	ed.					

21. Display the cluster port connectivity on each node:

network device-discovery show

cluster::*> network device-discovery show Local Discovered							
Node	Port	Device	Interface	Platform			
n1	 /cdp						
	e4a	C1	Ethernet1/7	N3K-C3232C			
	e4e	n2	e4e	FAS9000			
n2	/cdp						
	e4a	C1	Ethernet1/8	N3K-C3232C			
	e4e	n1	e4e	FAS9000			

22. Migrate clus2 to port e4a on the console of each node:

network interface migrate cluster -lif lif-name -source-node source-node-name -destination-node destination-node-name -destination-port destination-port-name

You must migrate each LIF to its home port individually as shown in the following example:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e4a
cluster::*> network interface migrate -vserver cluster -lif n2_clus2
-source-node n2 -destination-node n2 -destination-port e4a
```

23. Shut down cluster ports clus2 LIF on both nodes:

```
network port modify
```

The following example shows the specified ports being set to false, shutting the ports down on both nodes:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

24. Verify the cluster LIF status:

network interface show

<pre>cluster::*> network interface show -role cluster</pre>								
(network i	(network interface show)							
	Logical	Status	Network	Current				
Current Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
	_							
Cluster								
	n1_clus1	up/up	10.10.0.1/24	n1	e4a			
true								
	n1_clus2	up/up	10.10.0.2/24	n1	e4a			
false								
	n2_clus1	up/up	10.10.0.3/24	n2	e4a			
true								
	n2 clus2	up/up	10.10.0.4/24	n2	e4a			
false	_							
4 entries w	ere display	ed.						

25. Disconnect the cable from e4e on node n1.

You can refer to the running configuration and connect the first 40 GbE port on switch C2 (port 1/7 in this example) to e4e on node n1, using the appropriate cabling for the Nexus 3232C switch model.

26. Disconnect the cable from e4e on node n2.

You can refer to the running configuration and connect e4e to the next available 40 GbE port on C2, port 1/8, using the appropriate cabling for the Nexus 3232C switch model.

27. Enable all node-facing ports on C2.

The following example shows ports 1 through 30 being enabled on Nexus 3132Q-V cluster switches C1 and C2 using a configuration supported in RCF NX3232C RCF v1.0 24p10g 26p100g.txt:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

28. Enable the second cluster port, e4e, on each node:

```
network port modify
```

The following example shows the second cluster port e4e being brought up on each node:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> network port modify -node n2 -port e4e -up-admin true
```

29. For each node, revert all of the migrated cluster interconnect LIFs: network interface revert

The following example shows the migrated LIFs being reverted to their home ports.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

30. Verify that all of the cluster interconnect ports are now reverted to their home ports:

```
network interface show -role cluster
```

The Is Home column should display a value of true for all of the ports listed in the Current Port column. If the displayed value is false, the port has not been reverted.

<pre>cluster::*> network interface show -role cluster (network interface show)</pre>							
(Hecwork I		Status	Network	Current			
Current Is	1091001		11000011	oullone			
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port		
Home							
	_						
Cluster							
	n1_clus1	up/up	10.10.0.1/24	n1	e4a		
true	4 3 0	,	10 10 0 0 /01		4		
	nl_clus2	up/up	10.10.0.2/24	n1	e4e		
true	n2 clus1	11n/11n	10.10.0.3/24	n2	e4a		
true	IIZ_CIUSI	up/up	10.10.0.3/24	112	Cia		
CIUC	n2 clus2	up/up	10.10.0.4/24	n2	e4e		
true	_						
4 entries we	ere display	ed.					

31. Verify that all of the cluster interconnect ports are in the ${\tt up}$ state:

network port show -role cluster

32. Display the cluster switch port numbers through which each cluster port is connected to each node: network device-discovery show

cluster::*>	networ Local	k device-discovery s	how	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

33. Display discovered and monitored cluster switches:

system cluster-switch show

cluster::*> system cluster-switch show

Switch Type Address Model

C1 cluster-network 10.10.1.101 NX3232CV

Serial Number: FOX00001

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3) I6(1)

Version Source: CDP

C2 cluster-network 10.10.1.102

NX3232CV

Serial Number: FOX000002

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3)16(1)

Version Source: CDP 2 entries were displayed.

34. Verify that switchless cluster detection changed the switchless cluster option to disabled:

network options switchless-cluster show`

35. Ping the remote cluster interfaces and perform an RPC server check:

cluster ping-cluster -node node-name

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1 clus1 n1
                                10.10.0.1
                        e4a
                        e4e 10.10.0.2
Cluster n1 clus2 n1
Cluster n2 clus1 n2
                        e4a
                               10.10.0.3
Cluster n2 clus2 n2 e4e 10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s) ......
Detected 9000 byte MTU on 32 path(s):
   Local 10.10.0.1 to Remote 10.10.0.3
   Local 10.10.0.1 to Remote 10.10.0.4
   Local 10.10.0.2 to Remote 10.10.0.3
   Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

36. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

```
+system cluster-switch log setup-password
```

system cluster-switch log enable-collection

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: C1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

37. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Replace a Cisco Nexus 3232C cluster switch

You must be aware of certain configuration information, port connections and cabling requirements when you replace Cisco Nexus 3232C cluster switches.

You -ust verify the following conditions exist before installing the NX-OS software and RCFs on a Cisco Nexus cluster switch:

- Your system can support Cisco Nexus 3232C switches.
- The cluster must be fully functioning.
- You must have consulted the switch compatibility table on the Cisco Ethernet Switch page for the supported ONTAP, NX-OS, and RCF versions.



You should be aware there can be dependencies between command syntax in the RCF and NX-OS versions.

- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures.
- · You must have downloaded the applicable RCFs.

How to replace a Cisco Nexus 3232C cluster switch

You can nondisruptively replace a defective Cisco Nexus 3232C switch in a cluster by performing a specific sequence of tasks.

Before you begin

The existing cluster and network configuration must have the following characteristics:

• The Nexus 3232C cluster infrastructure must be redundant and fully functional on both switches.

The Cisco Ethernet Switches page has the latest RCF and NX-OS versions on your switches.

- All cluster ports must be in the up state.
- Management connectivity must exist on both switches.
- · All cluster logical interfaces (LIFs) must be in the up state and must not have been migrated.

The replacement Cisco Nexus 3232C switch must have the following characteristics:

- · Management network connectivity must be functional.
- Console access to the replacement switch must be in place.
- The appropriate RCF and NX-OS operating system image must be loaded onto the switch.
- Initial customization of the switch must be complete.

About this task

Procedure summary

- Display and migrate the cluster ports to switch C2 (Steps 1-7)
- Reconnect ISL cables from switch CL2 to switch C2, then migrate ISLs to switch CL1 and C2 (Steps 8-14)
- Revert all LIFs to originally assigned ports (Steps 15-18)
- Verify all ports and LIF are correctly migrated (Steps 19-21)

This procedure replaces the second Nexus 3232C cluster switch CL2 with the new 3232C switch C2. The

examples in this procedure use the following switch and node nomenclature:

- The four nodes are n1, n2, n3, and n4.
- n1_clus1 is the first cluster logical interface (LIF) connected to cluster switch C1 for node n1.
- n1 clus2 is the first cluster LIF connected to cluster switch CL2 or C2 for node n1.
- n1 clus3 is the second LIF connected to cluster switch C2 for node n1.-
- n1 clus4 is the second LIF connected to cluster switch CL1, for node n1.

The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.

The examples in this procedure use four nodes. Two of the nodes use four 10 GB cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40 GB cluster interconnect ports: e4a and e4e. See the Hardware Universe to verify the correct cluster ports for your platform.

This procedure describes the following scenario:

- The cluster initially has four nodes connected to two Nexus 3232C cluster switches, CL1 and CL2.
- You plan to replace cluster switch CL2 with C2 (steps 1 to 21):
 - On each node, you migrate the cluster LIFs connected to cluster switch CL2 to cluster ports connected to cluster switch CL1.
 - You disconnect the cabling from all ports on cluster switch CL2 and reconnect the cabling to the same ports on the replacement cluster switch C2.
 - You revert the migrated cluster LIFs on each node.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

+

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

1. Display information about the devices in your configuration:

network device-discovery show

		device-discovery sl Discovered	now	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3232C
	e0b	CL2	Ethernet1/1/1	N3K-C3232C
	e0c	CL2	Ethernet1/1/2	N3K-C3232C
	e0d	CL1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
	e0c	CL2	Ethernet1/1/4	N3K-C3232C
	e0d	CL1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3232C
	e4e	CL2	Ethernet1/7	N3K-C3232C
14	/cdp			
	_	CL1	Ethernet1/8	N3K-C3232C

- 2. Determine the administrative or operational status for each cluster interface.
 - a. Display the network port attributes:

network port show -role cluster

```
cluster::*> network port show -role cluster
(network port show)
Node: n1
Ignore
                                            Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
                                   up 9000 auto/10000 -
e0a
      Cluster
                   Cluster
e0b
       Cluster
                    Cluster
                                        9000 auto/10000 -
                                   up
```

e0c	Cluster	Cluster			0000	auto/10000	_
	Cluster	Cluster		up up		auto/10000 auto/10000	_
<u>-</u>	Cluster	Cluster		uр	9000	aut0/10000	_
Node: n2							
Ignore							
						Speed(Mbps)	Health
Health				- ' 1		7.1.1.70	
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a	Cluster	Cluster		up	9000	auto/10000	_
	Cluster	Cluster		up	9000		
	Cluster	Cluster		up	9000		
	Cluster			up	9000		
_				T			
Node: n3							
Ignore							
						Speed (Mbps)	Health
Health				- ' 1		7.1.1.70	~
Port Status	IPspace	Broadcast	Domain	Llnk	M.I.O	Admin/Oper	Status
e4a	Cluster	Cluster		up	9000	auto/40000	_
_				-			
e4e	Cluster	Cluster		up	9000	auto/40000	_
_							
Node: n4							
Ignore							
						Speed(Mbps)	Health
Health							
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
	Cluster	Cluster		up	9000	auto/40000	-
e4a						auto/40000	

b. Display information about the logical interfaces (LIFs):

network interface show -role cluster

	Logical	Status	Network	Current
Current				
		Admin/Oper	Address/Mask	Node
Port	Home			
Cluster	^			
0100001		up/up	10.10.0.1/24	n1
e0a	-	<u> </u>		
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	_	up/up	10.10.0.4/24	n1
e0d	true	,	10 10 0 5 /04	
-0-	_	up/up	10.10.0.5/24	n2
e0a	true	un /un	10.10.0.6/24	n2
e0b	true	ир/ ир	10.10.0.0/24	112
		up/up	10.10.0.7/24	n2
e0c	true	-1, -1		
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e0a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e0e	true	,	10 10 0 11 /0 /	
-0-	n4_clus1	up/up	10.10.0.11/24	n4
e0a	true	110/110	10 10 0 10/04	n /
e0e	n4_Clus2 true	up/up	10.10.0.12/24	n4
C0E	CIUC			

c. Display the discovered cluster switches:

system cluster-switch show

The following output example displays the cluster switches:

cluster::> system cluster-switch show Switch Type Address Model cluster-network 10.10.1.101 CL1 NX3232C Serial Number: FOX00001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)16(1)Version Source: CDP CL2 cluster-network 10.10.1.102 NX3232C Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)16(1)Version Source: CDP 2 entries were displayed.

- 3. Verify that the appropriate RCF and image are installed on the new Nexus 3232C switch and make any necessary site customizations.
 - a. Go to the NetApp Support Site.

mysupport.netapp.com

b. Go to the Cisco Ethernet Switches page and note the required software versions in the table.

Cisco Ethernet Switches

- c. Download the appropriate version of the RCF.
- d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then navigate to the **Download** page.
- e. Download the correct version of the image software from the Cisco® Cluster and Management Network Switch Reference Configuration File Download page.

Cisco® Cluster and Management Network Switch Reference Configuration File Download

4. Migrate the cluster LIFs to the physical node ports connected to the replacement switch C2:

network interface migrate -vserver Cluster -lif lif-name -source-node node-

name -destination-node node-name -destination-port port-name

You must migrate all the cluster LIFs individually as shown in the following example:

```
cluster::*> network interface migrate -vserver Cluster -lif n1 clus2
-source-node n1 -destination-
node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1 clus3
-source-node n1 -destination-
node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2 clus2
-source-node n2 -destination-
node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -destination-
node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 -destination-
node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4 clus2
-source-node n4 -destinationnode
n4 -destination-port e4a
```

5. Verify the status of the cluster ports and their home designations:

network interface show -role cluster

	Logical	Status	Network	Current	
Current Is Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
	· – – – – – – – – – – – – – – – – – – –				
Cluster		,		_	
true	n1_clus1	up/up	10.10.0.1/24	n1	e0a
	n1_clus2	up/up	10.10.0.2/24	n1	e0a
false	n1 clus3	up/up	10.10.0.3/24	n1	e0d
false	_				
true	n1_clus4	up/up	10.10.0.4/24	n1	e0d
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true	n2 clus2	up/up	10.10.0.6/24	n2	e0a
false	_				
false	n2_clus3	up/up	10.10.0.7/24	n2	e0d
	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true	n3 clus1	up/up	10.10.0.9/24	n3	e4a
true	_				
false	n3_clus2	up/up	10.10.0.10/24	n3	e4a
	n4_clus1	up/up	10.10.0.11/24	n4	e4a
true	n4 clus2	up/up	10.10.0.12/24	n4	e4a

^{6.} Shut down the cluster interconnect ports that are physically connected to the original switch CL2: network port modify -node node-name -port port-name -up-admin false

The following example shows the cluster interconnect ports are shut down on all nodes:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false cluster::*> network port modify -node n1 -port e0c -up-admin false cluster::*> network port modify -node n2 -port e0b -up-admin false cluster::*> network port modify -node n2 -port e0c -up-admin false cluster::*> network port modify -node n3 -port e4e -up-admin false cluster::*> network port modify -node n4 -port e4e -up-admin false
```

7. Ping the remote cluster interfaces and perform an RPC server check:

```
cluster ping-cluster -node node-name
```

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1 clus1 n1
                        e0a
                               10.10.0.1
Cluster n1 clus2 n1
                               10.10.0.2
                        e0b
Cluster n1 clus3 n1
                        e0c
                               10.10.0.3
                        e0d
                               10.10.0.4
Cluster n1 clus4 n1
Cluster n2 clus1 n2
                        e0a
                               10.10.0.5
Cluster n2 clus2 n2
                        e0b
                               10.10.0.6
Cluster n2 clus3 n2
                        e0c
                               10.10.0.7
Cluster n2 clus4 n2
                        e0d
                               10.10.0.8
Cluster n3 clus1 n4
                               10.10.0.9
                        e0a
Cluster n3 clus2 n3
                        e0e
                               10.10.0.10
Cluster n4 clus1 n4
                        e0a
                               10.10.0.11
                        e0e
                                10.10.0.12
Cluster n4 clus2 n4
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11
10.10.0.12 Cluster Vserver Id = 4294967293 Ping status:
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) ......
Detected 9000 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
   Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
   Local 10.10.0.1 to Remote 10.10.0.9
   Local 10.10.0.1 to Remote 10.10.0.10
   Local 10.10.0.1 to Remote 10.10.0.11
   Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
```

```
Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
    paths up, 0 paths down (udp check)
```

8. Shut down the ports 1/31 and 1/32 on cluster switch CL1.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1 (config-if-range) # shutdown
(CL1 (config-if-range) # exit
(CL1) (Config) # exit (CL1) #
```

- 9. Remove all the cables attached to the cluster switch CL2 and reconnect them to the replacement switch C2 for all the nodes.
- 10. Remove the inter-switch link (ISL) cables from ports e1/31 and e1/32 on cluster switch CL2 and reconnect them to the same ports on the replacement switch C2.
- 11. Bring up ISL ports 1/31 and 1/32 on the cluster switch CL1.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1(config-if-range) # no shutdown
(CL1(config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

12. Verify that the ISLs are up on CL1.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

Ports Eth1/31 and Eth1/32 should indicate (P), which means that the ISL ports are up in the port-channel:

13. Verify that the ISLs are up on cluster switch C2.

For more information on Cisco commands, see the guides listed in the Cisco Nexus 3000 Series NX-OS Command References.

14. On all nodes, bring up all the cluster interconnect ports connected to the replacement switch C2: network port modify -node node-name -port port-name -up-admin true

```
cluster::*> network port modify -node n1 -port e0b -up-admin true cluster::*> network port modify -node n1 -port e0c -up-admin true cluster::*> network port modify -node n2 -port e0b -up-admin true cluster::*> network port modify -node n2 -port e0c -up-admin true cluster::*> network port modify -node n3 -port e4e -up-admin true cluster::*> network port modify -node n4 -port e4e -up-admin true
```

15. Revert all the migrated cluster interconnect LIFs on all the nodes:

```
network interface revert -vserver cluster -lif lif-name
```

You must revert all the cluster interconnect LIFs individually as shown in the following example:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
Cluster::*> network interface revert -vserver cluster -lif n3_clus2
Cluster::*> network interface revert -vserver cluster -lif n4_clus2
```

16. Verify that the cluster interconnect ports are now reverted to their home:

```
network interface show
```

The following example shows that all the LIFs have been successfully reverted because the ports listed under the Current Port column have a status of true in the Is Home column. If a port has a value of false, the LIF has not been reverted.

	Logical	Status	Network	Current	
Current Is	-				
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true	n3_clus1	up/up	10.10.0.9/24	n3	e4a
true	n3_clus2	up/up	10.10.0.10/24	n3	e4e
true	n4_clus1	up/up	10.10.0.11/24	n4	e4a
true	n4 clus2	up/up	10.10.0.12/24	n4	e4e

17. Verify that the cluster ports are connected:

network port show -role cluster

```
cluster::*> network port show -role cluster
  (network port show)
```

Node: n1								
Ignore						Speed(Mbps)	Health	
Health								
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
Status								
 e0a	Cluster	Cluster		110	9000	auto/10000	_	
e0b	Cluster			up up		auto/10000 auto/10000		
e0c		Cluster		-		auto/10000		
e0d		Cluster		_		auto/10000		_
Coa	Olubect	Clubcci		αр	3000	440710000		
Node: n2								
Ignore								
II 1 + 1-						Speed (Mbps)	Health	
Health	T.D. a.a. a.a.	Description	Damaia	T	MODIT	7 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	0+-+	
Port Status	IPspace	Broadcast	Domain	ТТИК	MTO	Admin/Oper	Status	
								_
e0a	Cluster	Cluster		up	9000	auto/10000	-	
e0b	Cluster	Cluster		up	9000	auto/10000	-	
e0c	Cluster	Cluster		up	9000	auto/10000	_	
e0d	Cluster	Cluster		up	9000	auto/10000	-	-
Node: n3								
Ignore								
Health						Speed (Mbps)	Health	
Port	IPspace	Broadcast	Domain	Link	МТП	Admin/Oper	Status	
Status	IIBpace	Dioadease	Domain		1110	namin, open	beacab	
e4a	Cluster	Cluster		up	9000	auto/40000	-	
e4e	Cluster	Cluster		up	9000	auto/40000	-	-
Node: n4								
Ignore								
II o o l + l·						Speed (Mbps)	неаlth	
Health	TPanaga	Prondenst	Domain	Tiple	МПТТ	Admin/Onor	Status	
Status	IPspace	DIOAUCAST	DOMINATI	ТТПК	MIO	Admin/Oper	SLALUS	

```
e4a Cluster Cluster up 9000 auto/40000 -
e4e Cluster Cluster up 9000 auto/40000 -
12 entries were displayed.
```

18. Ping the remote cluster interfaces and perform an RPC server check:

```
cluster ping-cluster -node node-name
```

The following example shows node n1 being pinged and the RPC status indicated afterward:

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1 clus1 n1
                         e0a
                                10.10.0.1
Cluster n1 clus2 n1
                                10.10.0.2
                         e0b
Cluster n1 clus3 n1
                         e0c
                                10.10.0.3
Cluster n1 clus4 n1
                         e0d
                               10.10.0.4
Cluster n2 clus1 n2
                                10.10.0.5
                        e0a
Cluster n2 clus2 n2
                        e0b
                               10.10.0.6
Cluster n2 clus3 n2
                        e0c
                                10.10.0.7
Cluster n2 clus4 n2
                         e0d
                                10.10.0.8
Cluster n3 clus1 n3
                        e0a
                               10.10.0.9
Cluster n3 clus2 n3
                         e0e
                                10.10.0.10
Cluster n4 clus1 n4
                         e0a
                               10.10.0.11
Cluster n4 clus2 n4
                                10.10.0.12
                         e0e
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293 Ping status:
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) ......
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
   Local 10.10.0.1 to Remote 10.10.0.6
   Local 10.10.0.1 to Remote 10.10.0.7
   Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
   Local 10.10.0.1 to Remote 10.10.0.10
   Local 10.10.0.1 to Remote 10.10.0.11
   Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
```

```
Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
   paths up, 0 paths down (udp check)
```

19. Display the information about the devices in your configuration by entering the following commands:

You can execute the following commands in any order:

```
network device-discovery shownetwork port show -role clusternetwork interface show -role cluster
```

° system cluster-switch show

	Local	Discovered	_	
Node	Port	Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1
Ignore
                                             Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster Cluster up 9000 auto/10000 -
                   Cluster up 9000 auto/10000 - Cluster up 9000 auto/10000 -
       Cluster Cluster
Cluster Cluster
e0b
e0c
       Cluster Cluster
                                   up 9000 auto/10000 -
e0d
Node: n2
```

Ignore							
Health						Speed (Mbps)	Health
Port	IPspace	Broadcast	Domain	T.ink	МТІІ	Admin/Oner	Status
Status	115pace	broadcase	DOMATH	ПТПК	MIO	Admin Open	Scacus
							_
e0a	Cluster	Cluster		up	9000	auto/10000	_
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d	Cluster	Cluster		up	9000	auto/10000	-
_							
Node: n3							
Ignore							
Heel+h						Speed (Mbps)	Health
Health	IPspace	Prondenst	Domain	Tink	MITIT	Admin/Oper	C+ 2+11C
Status	irspace	DIOaucast	DOMATH	ПТПК	MIO	Admitity Oper	Status
	Cluster			_		auto/40000	-
e4e	Cluster	Cluster		up	9000	auto/40000	-
- Node: n4							
11000. 111							
Ignore							
II 1 + 1-						Speed (Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	МТІІ	Admin/Oper	Status
Status	110000	Diddedoc	Domail		1110	110m211/OPCI	204045
	Cluster			_		auto/40000	
e4e	Cluster	Cluster		up	9000	auto/40000	-
12 entrie	s were display	yed.					

cluster	::*> network in	nterface sho	w -role cluster	
	Logical	Status	Network	Current
Current	Is			
		Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
	nm1_clus1	up/up	10.10.0.1/24	n1
e0a	true	,	10.10.0.0/01	
e0b	nl_clus2 true	up/up	10.10.0.2/24	n1
600		מנו/מנו	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
- 0 -	_	up/up	10.10.0.5/24	n2
e0a	true n2 clus2	up/up	10.10.0.6/24	n2
e0b	true	αρ/ αρ	10.10.0.0721	112
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
0.1	_	up/up	10.10.0.8/24	n2
e0d	true	11n / 11n	10.10.0.9/24	n3
e4a	true	ир/ ир	10.10.0.3/24	113
		up/up	10.10.0.10/24	n3
e4e	true			
	-	up/up	10.10.0.11/24	n4
e4a	true		10 10 0 10/04	n 1
e4e	n4_clus2 true	up/up	10.10.0.12/24	n4
	ries were disp	layed.		
		1		

cluster::*> system cluster-switch show

Switch Type Address Model

CL1 cluster-network 10.10.1.101 NX3232C

Serial Number: FOX000001

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3)16(1)

Version Source: CDP

CL2 cluster-network 10.10.1.102 NX3232C

Serial Number: FOX000002

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3) I6(1)

Version Source: CDP

C2 cluster-network 10.10.1.103 NX3232C

Serial Number: FOX000003

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3)I6(1) Version Source: CDP 3 entries were

displayed.

20. Delete the replaced cluster switch CL2 if it has not been removed automatically:

system cluster-switch delete -device cluster-switch-name

21. Verify that the proper cluster switches are monitored: system cluster-switch show

The following example shows the cluster switches are monitored because the Is Monitored state is true.

cluster::> system cluster-switch show

Switch Type Address Model

CL1 cluster-network 10.10.1.101 NX3232C

Serial Number: FOX00001

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3) I6(1)

Version Source: CDP

C2 cluster-network 10.10.1.103 NX3232C

Serial Number: FOX000002

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

7.0(3)16(1)

Version Source: CDP

2 entries were displayed.

22. Enable the cluster switch health monitor log collection feature for collecting switch-related log files:

system cluster-switch log setup-password

system cluster-switch log enable-collection

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
CL1
C2
cluster::*> system cluster-switch log setup-password
Enter the switch name: CL1
**RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log setup-password
Enter the switch name: C2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster::*>
```



If any of these commands return an error, contact NetApp support.

23. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Related information

Cisco Ethernet Switch description page

Hardware Universe

Replace a Cisco Nexus 3232C storage switch

You must be aware of certain configuration information, port connections and cabling requirements when you replace Cisco Nexus 3232C storage switches.

You must verify the following conditions exist before installing the NX-OS software and RCFs on a Cisco Nexus storage switch:

- Your system can support Cisco Nexus 3232C storage switches.
- You must have consulted the switch compatibility table on the Cisco Ethernet Switch page for the supported ONTAP, NX-OS, and RCF versions.



You should be aware there can be dependencies between command syntax in the RCF and NX-OS versions.

- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures at Cisco Nexus 3000 Series Switches.
- · You must have downloaded the applicable RCFs.

Steps to replace a Cisco Nexus 3232C storage switch

You can nondisruptively replace a defective Cisco Nexus 3232C storage switch by performing a specific sequence of tasks.

Before you begin

The existing network configuration must have the following characteristics:

- The Cisco Ethernet Switches page has the latest RCF and NX-OS versions on your switches.
- Management connectivity must exist on both switches.



Make sure that all troubleshooting steps have been completed to confirm that your switch needs replacing.

The replacement Cisco Nexus 3232C switch must have the following characteristics:

- · Management network connectivity must be functional.
- Console access to the replacement switch must be in place.
- The appropriate RCF and NX-OS operating system image must be loaded onto the switch.
- Initial customization of the switch must be complete.

Procedure summary:

- Confirm the switch to be replaced is S2 (Steps 1-5)
- Disconnect the cables from switch S2 (Step 6)
- Reconnect the cables to switch NS2 (Step 7)
- Verify all device configurations on switch NS2 (Steps 8-10)

- This procedure replaces the second Nexus 3232C storage switch S2 with the new 3232C switch NS2.
- The two nodes are node1 and node2.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Check on the health status of the storage node ports to make sure that there is connection to storage switch S1:

storage port show -port-type ENET

storage::*> storag	e por	t show	-port-ty	pe ENE	Γ		
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

 Verify that storage switch S1 is available: network device-discovery show

storage::*>	networ	k device-discovery show		
Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
				-
node1/cdp				
	e3a	S1	Ethernet1/1	NX3232C
	e4a	node2	e4a	AFF-A700
	e4e	node2	e4e	AFF-A700
node1/lldp				
	e3a	S1	Ethernet1/1	_
	e4a	node2	e4a	_
	e4e	node2	e4e	_
node2/cdp				
	e3a	S1	Ethernet1/2	NX3232C
	e4a	node1	e4a	AFF-A700
	e4e	node1	e4e	AFF-A700
node2/11dp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	_
	e4e	node1	e4e	_

4. Run the show 11dp neighbors command on the working switch to confirm that you can see both nodes and all shelves:

show lldp neighbors

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID
                        Local Intf
                                         Hold-time Capability Port ID
node1
                        Eth1/1
                                         121
                                                    S
                                                                 еЗа
node2
                        Eth1/2
                                         121
                                                    S
                                                                 еЗа
SHFGD2008000011
                        Eth1/5
                                         121
                                                    S
                                                                 e0a
SHFGD2008000011
                        Eth1/6
                                         120
                                                    S
                                                                 e0a
SHFGD2008000022
                        Eth1/7
                                         120
                                                    S
                                                                 e0a
SHFGD2008000022
                        Eth1/8
                                         120
                                                    S
                                                                 e0a
```

5. Verify the shelf ports in the storage system:

storage shelf port show -fields remote-device, remote-port

storage::*> storage shelf port show -fields remote-device, remote-port shelf id remote-port remote-device ------_____ 3.20 0 Ethernet1/5 S1 3.20 1 3.20 2 Ethernet1/6 S1 3.20 3 3.30 0 Ethernet1/7 S1 3.20 1 -3.30 2 Ethernet1/8 S1 3.20 3 -

- 6. Remove all cables attached to storage switch S2.
- 7. Reconnect all cables to the replacement switch NS2.
- 8. Recheck the health status of the storage node ports: storage port show -port-type ENET

storage::*> stor	age por	t show	-port-ty	pe ENE	Г		
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

Verify that both switches are available: network device-discovery show

-		k device-discovery show		
Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node1/cdp				
	e3a	S1	Ethernet1/1	NX3232C
	e4a	node2	e4a	AFF-A700
	e4e	node2	e4e	AFF-A700
	e7b	NS2	Ethernet1/1	NX3232C
node1/lldp				
	e3a	S1	Ethernet1/1	_
	e4a	node2	e4a	_
	e4e	node2	e4e	_
	e7b	NS2	Ethernet1/1	-
node2/cdp				
	e3a	S1	Ethernet1/2	NX3232C
	e4a	node1	e4a	AFF-A700
	e4e	node1	e4e	AFF-A700
	e7b	NS2	Ethernet1/2	NX3232C
node2/11dp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-
	e7b	NS2	Ethernet1/2	-

10. Verify the shelf ports in the storage system:

storage shelf port show -fields remote-device, remote-port

11. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Upgrade a Cisco Nexus 3232C storage switch

The Cisco NX-OS software and reference configuration files (RCFs) can be upgraded on Cisco Nexus 3232C storage switches.

Before you begin

The following conditions must exist before you upgrade the NX-OS software and RCFs on the storage switch:

- The switch must be fully functioning (there should be no errors in the logs or similar issues).
- You must have checked or set your desired boot variables in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.

If you need to change the boot variables to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.

- You must have referred to the appropriate software and upgrade guides available on the Cisco Nexus 3000 Series Switches page for complete documentation on the Cisco storage upgrade and downgrade procedures.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Ethernet Switches page.

Procedure summary:

- I. Check the health status of switches and ports (Steps 1-4)
- II. Copy the RCF to Cisco switch S2 (Steps 5 8)
- III. Download the NX-OS image to Cisco switch S2 and reboot (Steps 9 12)
- IV. Recheck the health status of switches and ports (Steps 13 15)
- V. Repeat Steps 1- 17 for Cisco switch S1.

The examples in this procedure use two nodes; node1 with two storage ports and node2 with two storage ports. See the Hardware Universe to verify the correct storage ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two storage switches are S1 and S2.
- The nodes are node1 and node2.



The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Check that the storage switches are available:

system switch ethernet show

```
storage::*> system switch ethernet show
                                       Address
                                                      Model
Switch
                        Type
__________
S1
                        storage-network 172.17.227.5 NX3232C
    Serial Number: FOC221206C2
     Is Monitored: true
         Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                 9.3(3)
   Version Source: CDP
S2
                        storage-network 172.17.227.6 NX3232C
    Serial Number: FOC220443LZ
     Is Monitored: true
          Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                 9.3(3)
   Version Source: CDP
2 entries were displayed.
storage::*>
```

3. Verify that the node ports are healthy and operational:

storage port show -port-type ENET

storage::*> storag	e por	t show	-port-t	/pe ENE'	Γ		
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

4. Check that there are no storage switch or cabling issues with the cluster:

system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

5. Copy the RCF on switch S2 to the switch bootflash using one of the following transfer protocols: FTP, HTTP, TFTP, SFTP, or SCP.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows HTTP being used to copy an RCF to the bootflash on switch S2:

```
S2# copy http://172.16.10.1//cfg/Nexus 3232C RCF v1.6-Storage.txt
bootflash: vrf management
        % Received % Xferd Average Speed
% Total
                                           Time
                                                  Time
                                                           Time
Current
                            Dload
                                    Upload Total
                                                  Spent
                                                           Left
Speed
           3254
 100
                100
                            3254
                                    0
                                           0
                                                  8175
                                                           0 --:
--:-- 8301
Copy complete, now saving to disk (please wait) ...
Copy complete.
S2#
```

6. Apply the RCF previously downloaded to the bootflash:

copy bootflash:

The following example shows the RCF file <code>Nexus_3232C_RCF_v1.6-Storage.txt</code> being installed on switch S2:

S2# copy Nexus 3232C RCF v1.6-Storage.txt running-config echo-commands

7. Verify that the RCF file is the correct newer version:

show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

- The RCF banner
- The node and port settings
- Customizations

The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.



In the banner output from the show banner motd command, you must read and follow the instructions in the **IMPORTANT NOTES** section to ensure the proper configuration and operation of the switch.

```
S2# show banner motd
******************
* NetApp Reference Configuration File (RCF)
* Switch : Cisco Nexus 3232C
* Filename : Nexus 3232C RCF v1.6-Storage.txt
* Date : Oct-20-2020
* Version : v1.6
* Port Usage : Storage configuration
* Ports 1-32: Controller and Shelf Storage Ports
* Ports 33-34: Disabled
* IMPORTANT NOTES*
* - This RCF utilizes QoS and requires TCAM re-configuration, requiring
RCF
   to be loaded twice with the Storage Switch rebooted in between.
* - Perform the following 4 steps to ensure proper RCF installation:
   (1) Apply RCF first time, expect following messages:
       - Please save config and reload the system...
       - Edge port type (portfast) should only be enabled on ports...
       - TCAM region is not configured for feature QoS class IPv4
ingress...
    (2) Save running-configuration and reboot Cluster Switch
    (3) After reboot, apply same RCF second time and expect following
messages:
       - % Invalid command at '^' marker
       - Syntax error while parsing...
   (4) Save running-configuration again
*****************
*****
S2#
```



When applying the RCF for the first time, the **ERROR: Failed to write VSH commands** message is expected and can be ignored.

8. After you verify that the software versions and switch settings are correct, copy the running-config file to the startup-config file on switch S2.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

The following example shows the running-config file successfully copied to the startup-config file:

```
S2# copy running-config startup-config
[############################# 100% Copy complete.
```

- 9. Download the NX-OS image to switch S2.
- 10. Install the system image so that the new version will be loaded the next time switch S2 is rebooted.

The switch will be reboot in 10 seconds with the new image as shown in the following output:

```
S2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[############### 100% -- SUCCESS
Verifying image type.
[[############### 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[############### 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[############### 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
reset default upgrade is not
          yes disruptive
hitless
Images will be upgraded according to following table:
Module Image
                              Running-Version(pri:alt)
New-Version Upg-Required
```

```
______
                                                 9.3(3)
    1
            nxos
9.3(4)
               yes
            bios v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)
                           no
Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n] y
input string too long
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.
S2#
```

11. Save the configuration.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command References.

You are prompted to reboot the system as shown in the following example:

```
S2# copy running-config startup-config
[############################### 100% Copy complete.
S2# reload
This command will reboot the system. (y/n)? [n] y
```

12. Confirm that the new NX-OS version number is on the switch:

```
S2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
otherwise stated, there is no warranty, express or implied, including
but not
limited to warranties of merchantability and fitness for a particular
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 08.38
 NXOS: version 9.3(4)
 BIOS compile time: 05/29/2020
 NXOS image file is: bootflash:///nxos.9.3.4.bin
 NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]
Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FOC20291J6K
  Device name: S2
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020
  Reason: Reset due to upgrade
  System version: 9.3(3)
  Service:
```

```
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
S2#
```

13. Recheck that the storage switches are available after the reboot:

system switch ethernet show

```
storage::*> system switch ethernet show
Switch
                                           Address
                                                            Model
                          Type
_____
S1
                          storage-network 172.17.227.5 NX3232C
    Serial Number: FOC221206C2
     Is Monitored: true
           Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(4)
   Version Source: CDP
S2
                          storage-network 172.17.227.6 NX3232C
    Serial Number: FOC220443LZ
     Is Monitored: true
           Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(4)
   Version Source: CDP
2 entries were displayed.
storage::*>
```

14. Verify that the switch ports are healthy and operational after the reboot:

storage port show -port-type ENET

storage::*> storag	e por	t show	-port-ty	pe ENE	Г		
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

15. Recheck that there are no storage switch or cabling issues with the cluster: system health alert show -instance

```
\verb|storage::*> \verb|system| | health | alert | show - instance \\ | There | are | no | entries | matching | your | query.
```

- 16. Repeat the procedure to upgrade the NX-OS software and RCF on switch S1.
- 17. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Cisco Nexus 9336C-FX2 switches

Cisco 9336C-FX2 switch overview

If you want to build ONTAP clusters with more than two nodes, you need two supported cluster network switches. You can use additional management switches, which are optional.

You can install the Cisco Nexus 9336C-FX2 switch (X190200/X190210) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following table lists the part number and description for the 9336C-FX2 switch, fans, and power supplies:

Part number	Description
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Accessory Kit X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100W PSU - Port side exhaust airflow
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100W PSU - Port side Intake airflow
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, Port side exhaust airflow
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, Port side intake airflow

Other supported switches

Nexus 3232C

You can install the Cisco Nexus 3232C switch (X190100) NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

Nexus 3132Q-V

You can install the Cisco Nexus 3132Q-V switch (X190001) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following cluster switches are no longer available from NetApp, but will be supported by Cisco for a limited time:

Nexus 5596UP/5596T

You can install the Cisco Nexus 5596UP switch (X1967-R6) or 5596T (X1989-R6) in a NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

The Nexus 5596UP switch also supports one or two 16-port expansion modules (X1988-R6).

The Nexus 5596T switch is only supported as a cluster interconnect switch for the FAS2520 and is intended to be used for performing nondisruptive hardware upgrades.

End of Availability details.

Install a Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet

You can install the Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.

About this task

You must have reviewed the initial preparation requirements, kit contents, and safety precautions.

Cisco Nexus 9000 Series Hardware Installation Guide

- For each switch, you must supply the eight 10-32 or 12-24 screws and clip nuts to mount the brackets and slider rails to the front and rear cabinet posts.
- You must use the Cisco standard rail kit to install the switch in a NetApp cabinet.



The jumper cords are not included with the pass-through kit and should be included with your switches. If they were not shipped with the switches, you can order them from NetApp (part number X1558A-R6).

Steps

1. Install the pass-through blanking panel in the NetApp cabinet.

The pass-through panel kit is available from NetApp (part number X8784-R6).

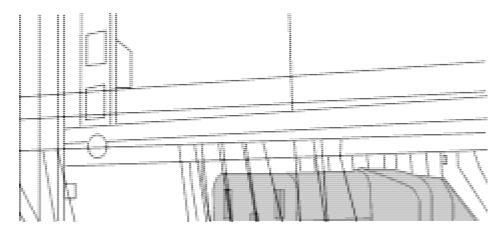
The NetApp pass-through panel kit contains the following hardware:

- One pass-through blanking panel
- Four 10-32 x .75 screws
- Four 10-32 clip nuts
 - a. Determine the vertical location of the switches and blanking panel in the cabinet.

In this procedure, the blanking panel will be installed in U40.

- b. Install two clip nuts on each side in the appropriate square holes for front cabinet rails.
- c. Center the panel vertically to prevent intrusion into adjacent rack space, and then tighten the screws.

d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



- i. Female connector of the jumper cord.
- 2. Install the rack-mount brackets on the Nexus 9336C-FX2 switch chassis.
 - a. Position a front rack-mount bracket on one side of the switch chassis so that the mounting ear is aligned with the chassis faceplate (on the PSU or fan side), and then use four M4 screws to attach the bracket to the chassis.

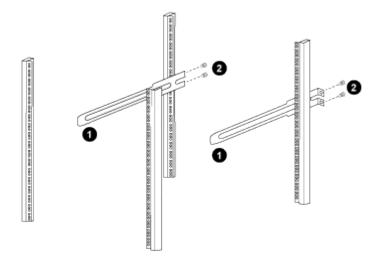


- b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.
- c. Install the rear rack-mount bracket on the switch chassis.
- d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.
- 3. Install the clip nuts in the square hole locations for all four IEA posts.



The two 9336C-FX2 switches will always be mounted in the top 2U of the cabinet RU41 and 42.

- 4. Install the slider rails in the cabinet.
 - a. Position the first slider rail at the RU42 mark on the back side of the rear left post, insert screws with the matching thread type, and then tighten the screws with your fingers.



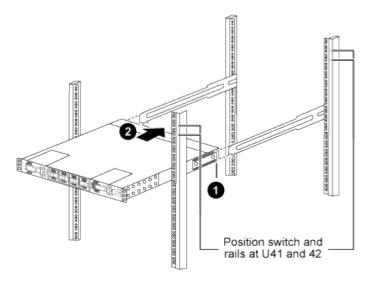
- i. As you gently slide the slider rail, align it to the screw holes in the rack.
- ii. Tighten the screws of the slider rails to the cabinet posts.
- b. Repeat step 4a for the right side rear post.

- c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.
- 5. Install the switch in the cabinet.



This step requires two people: one person to support the switch from the front and another to guide the switch into the rear slider rails.

a. Position the back of the switch at RU41.



- i. As the chassis is pushed toward the rear posts, align the two rear rack-mount guides with the slider rails.
- ii. Gently slide the switch until the front rack-mount brackets are flush with the front posts.
- b. Attach the switch to the cabinet.



- i. With one person holding the front of the chassis level, the other person should fully tighten the four rear screws to the cabinet posts.
- c. With the chassis now supported without assistance, fully tighten the front screws to the posts.
- d. Repeat steps 5a through 5c for the second switch at the RU42 location.



By using the fully installed switch as a support, it is not necessary to hold the front of the second switch during the installation process.

- 6. When the switches are installed, connect the jumper cords to the switch power inlets.
- 7. Connect the male plugs of both jumper cords to the closest available PDU outlets.



To maintain redundancy, the two cords must be connected to different PDUs.

8. Connect the management port on each 9336C-FX2 switch to either of the management switches (if ordered) or connect them directly to your management network.

The management port is the upper-right port located on the PSU side of the switch. The CAT6 cable for each switch needs to be routed through the pass-through panel after the switches are installed to connect to the management switches or management network.

Set up

Set up the switches

If you do not already have the required configuration information and documentation, you need to gather that information before setting up your cluster and management network switches.

- You must have access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- You must have the required cluster network and management network switch documentation.

See Required documentation for more information.

• You must have the required controller documentation and ONTAP documentation.

NetApp documentation

- You must have the applicable licenses, network and configuration information, and cables.
- You must have the completed cabling worksheets.



Due to the complexity that can result from illustrating layers of cabling, this guide does not provide cabling graphics. This guide does provide sample worksheets with recommended port assignments and blank worksheets that you can use to set up your cluster.



For more information refer to the Hardware Universe.

 All Cisco cluster network and management network switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software but do not have the RCFs loaded.



You must download the applicable NetApp cluster network and management network RCFs from the NetApp Support Site at mysupport.netapp.com for the switches that you receive.

 In addition, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for the 92300YC cluster switches. See Installing the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches for details.

Steps

1. Rack the cluster network and management network switches and controllers.

If you are installing your	Then
Cisco Nexus 9336C-FX2 in a NetApp system cabinet	See the <i>Installing a Cisco Nexus</i> 9336C-FX2 cluster switch and pass-through panel in a NetApp cabinet guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3232C in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.
Cisco Nexus 5596UP/5596T in a NetApp system cabinet	See the Installing a Cisco Nexus 5596 cluster switch and pass- through panel in a NetApp cabinet guide for instructions to install the switch in a NetApp cabinet.

- 2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheets.
- 3. Power on the cluster network and management network switches and controllers.
- 4. Perform an initial configuration of the cluster network switches based on information provided in Required configuration information.
- 5. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
- 6. Check the version on the cluster network switches, and if necessary, download the NetApp-supported version of the software to the switches.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Cluster Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and the instructions from the Cisco Ethernet Switches page.

7. Check the software version on the network switches and, if necessary, download the NetApp-supported version of the software to the switches. If you have your own switches, refer to the Cisco site.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Management Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and instructions from the Cisco Ethernet Switches page.

Related information

Required cluster configuration information

Required documentation

Sample and blank cabling worksheets

Required cluster configuration information

To configure your cluster, you need the appropriate number and type of cables and cable connectors for your switches. Depending on the type of switch you are initially configuring, you need to connect to the switch console port with the included console cable; you also need to provide specific network information.

Required network information for all switches

You need the following network information for all switch configurations:

- · IP subnet for management network traffic
- · Host names and IP addresses for each of the storage system controllers and all applicable switches
- Most storage system controllers are managed through the e0M interface by connecting to the Ethernet service port (wrench icon). On AFF A800 and AFF A700 systems, the e0M interface uses a dedicated Ethernet port.

Refer to the Hardware Universe for latest information.

Required network information for Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches

For the Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches, you need to provide applicable responses to the following initial setup questions when you first boot the switch. Your site's security policy defines the responses and services to enable.

Abort Auto Provisioning and continue with normal setup? (yes/no)

Respond with yes. The default is no.

• Do you want to enforce secure password standard? (yes/no)

Respond with **yes**. The default is yes.

• Enter the password for admin:

The default password is "admin"; you must create a new, strong password. A weak password can be rejected.

Would you like to enter the basic configuration dialog? (yes/no)

Respond with **yes** at the initial configuration of the switch.

Create another login account? (yes/no)

Your answer depends on your site's policies on alternate administrators. The default is **no**.

Configure read-only SNMP community string? (yes/no)

Respond with no. The default is no.

• Configure read-write SNMP community string? (yes/no)

Respond with **no**. The default is no.

• Enter the switch name.

The switch name is limited to 63 alphanumeric characters.

• Continue with Out-of-band (mgmt0) management configuration? (yes/no)

Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip address.

Configure the default-gateway? (yes/no)

Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.

Configure advanced IP options? (yes/no)

Respond with **no**. The default is no.

• Enable the telnet service? (yes/no)

Respond with **no**. The default is no.

• Enabled SSH service? (yes/no)

Respond with **yes**. The default is yes.



SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.

- Enter the type of SSH key you want to generate (dsa/rsa/rsa1). The default is rsa.
- Enter the number of key bits (1024-2048).
- Configure the NTP server? (yes/no)

Respond with **no**. The default is no.

• Configure default interface layer (L3/L2):

Respond with **L2**. The default is L2.

Configure default switch port interface state (shut/noshut):

Respond with **noshut**. The default is noshut.

• Configure CoPP system profile (strict/moderate/lenient/dense):

Respond with **strict**. The default is strict.

• Would you like to edit the configuration? (yes/no)

You should see the new configuration at this point. Review and make any necessary changes to the

configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.

• Use this configuration and save it? (yes/no)

Respond with **yes** to save the configuration. This automatically updates the kickstart and system images.



If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

For more information about the initial configuration of your switch, see the following guides:

Cisco Nexus 9336C-FX2 Installation and Upgrade Guides

Cisco Nexus 92300YC Installation and Upgrade Guides

Cisco Nexus 5000 Series Hardware Installation Guide

Cisco Nexus 3000 Series Hardware Installation Guide

Install the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches

You can use this procedure to install the applicable configuration file for cluster switch health monitoring of Nexus 92300YC cluster switches. In ONTAP releases 9.5P7 and earlier and 9.6P2 and earlier, you must download the cluster switch health monitor configuration file separately. In ONTAP releases 9.5P8 and later, 9.6P3 and later, and 9.7 and later, the cluster switch health monitor configuration file is bundled with ONTAP.

Before you setup the switch health monitor for 92300YC cluster switches, you must ensure that the ONTAP cluster is up and running.



It is advisable to enable SSH in order to use all features available in CSHM.

- 1. Download the cluster switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the NetApp Software download page.
 - a. On the Software download page, select Switch Health Monitor Configuration Files
 - b. Select Platform = **ONTAP** and click **Go!**
 - c. On the Switch Health Monitor Configuration Files for ONTAP page, click View & Download
 - d. On the Switch Health Monitor Configuration Files for ONTAP Description page, click **Download** for the applicable cluster switch model, for example: **Cisco Nexus 92300YC**
 - e. On the End User License Agreement page, click Accept
 - f. On the Switch Health Monitor Configuration Files for ONTAP Download page, select the applicable configuration file, for example, Cisco_Nexus_92300YC.zip
- 2. Upload the applicable zip file to your internal web server where the IP address is X.X.X.X.

For an internal web server IP address of 192.168.2.20 and assuming a /usr/download directory exists, you can upload your zip file to your web server using scp:

```
% scp Cisco_Nexus_92300YC.zip
admin@192.168.2.20:/usr/download/Cisco_Nexus_92300YC.zip
```

3. Access the advanced mode setting from one of the ONTAP systems in the cluster, using the command setprivilege advanced:

```
cluster1::> set -privilege advanced
```

4. Run the switch health monitor configure command system cluster-switch configure-health-monitor -node * -package-url X.X.X.X/location to download zip file:

```
cluster1::> system cluster-switch configure-health-monitor -node *
-package-url 192.168.2.20/usr/download/Cisco_Nexus_92300YC.zip
```

- 5. Verify that the command output contains the text string "downloaded package processed successfully". If an error occurs, contact NetApp support.
- 6. Run the command system cluster-switch show on the ONTAP system and ensure that the cluster switches are discovered with the monitored field set to "True".

```
cluster1::> system cluster-switch show
```



If at any time you revert to an earlier version of ONTAP, you will need to install the CSHM configuration file again to enable switch health monitoring of 92300YC cluster switches.

Required documentation

You need specific switch and controller documentation to set up your ONTAP cluster.

Required documentation for cluster network switches

To set up the Cisco Nexus 9336C-FX2 and 92300YC switches, you need the following documentation from the Cisco Nexus 9000 Series Switches Support page:

Document title	Description
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.

Document title	Description
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

To set up the Cisco Nexus 3232C and 3132Q-V switches, you need the following documentation from the Cisco Nexus 3000 Series Switches Support page:

Document title	Description
Nexus 3000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 3000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 3000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.

Document title	Description
Cisco Nexus 3000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.
Nexus 3000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 3000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 3000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 3000 series switches.

To set up the Cisco Nexus 5596 switch, you need the following documents from Cisco Nexus 5000 Series Switches Support page:

Document title	Description
Nexus 5000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 5000 Series Switch Software Configuration Guide (choose the guide for the software you are using)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide	Provides information about how to downgrade the switch to the supported ONTAP switch software, if necessary.
Cisco Nexus 5000 Series NX-OS Command Reference Master Index	Provides an alphabetical list of all the commands supported for a specific NX-OS release.
Cisco Nexus 5000 and Nexus 2000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 5000 switches.
Nexus 5000 Series NX-OS System Message Reference	Describes troubleshooting information.

Document title	Description
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000 Series, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 5000 series switches.

Required documentation for supported ONTAP systems

To set up an ONTAP system, you need the following documents for your version of the operating system from the ONTAP 9 Documentation Center.

Name	Description
Controller-specific Installation and Setup Instructions	Describes how to install NetApp hardware.
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.
Hardware Universe	Provides NetApp hardware configuration and compatibility information.

Rail kit and cabinet documentation

To install a Cisco switch in a NetApp cabinet, see the following hardware documentation:

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet	Describes how to install a Cisco Nexus 3232C switch in a four-post NetApp cabinet.
Installing a Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 3132Q-V switch in a four-post NetApp cabinet.
Installing a Cisco Nexus 5596 switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 5596 switch in a NetApp cabinet.

Considerations for using Smart Call Home

Smart Call Home monitors the hardware and software components on your network, to generate an email-based notification of critical system conditions. When an event occurs on your device, Smart Call Home raises an alert to all the recipients that are configured in your destination profile.

You must configure a cluster network switch to communicate using email with the Smart Call Home system. You can optionally set up your cluster network switch to take advantage of Cisco's embedded Smart Call Home support feature.

Before you can use Smart Call Home feature, you need to be aware of the following considerations:

- An email server must be in place.
- The switch must have IP connectivity to the email server.
- The contact name (SNMP server contact), phone number, and street address information must be configured.
- This is required to determine the origin of messages received.
- A CCO ID must be associated with an appropriate Cisco SMARTnet Service contract for your company.
- Cisco SMARTnet Service must be in place for the device to be registered.

The Cisco support site contains information about the commands to configure Smart Call Home.

Cisco support site

Sample and blank cabling worksheets

The sample cabling worksheets provide examples of recommended port assignments from the switches to the controllers. The blank worksheets provide a template that you can use in setting up your cluster.

Cisco Nexus 9336C-FX2 cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10GbE node 1	1	4x10GbE node 1
2	4x10GbE node 2	2	4x10GbE node 2
3	4x10GbE node 3	3	4x10GbE node 3
4	4x25GbE node 4	4	4x25GbE node 4
5	4x25GbE node 5	5	4x25GbE node 5
6	4x25GbE node 6	6	4x25GbE node 6

Cluster switch A		Cluster switch B	
7	4x100GbE node 7	7	4x100GbE node 7
8	4x100GbE node 8	8	4x100GbE node 8
9	4x100GbE node 9	9	4x100GbE node 9
10	4x100GbE node 10	10	4x100GbE node 10
11	4x100GbE node 11	11	4x100GbE node 11
12	4x100GbE node 12	12	4x100GbE node 12
13	4x100GbE node 13	13	4x100GbE node 13
14	4x100GbE node 14	14	4x100GbE node 14
15	4x100GbE node 15	15	4x100GbE node 15
16	4x100GbE node 16	16	4x100GbE node 16
17	4x100GbE node 17	17	4x100GbE node 17
18	4x100GbE node 18	18	4x100GbE node 18
19	4x100GbE node 19	19	4x100GbE node 19
20	4x100GbE node 20	20	4x100GbE node 20
21	4x100GbE node 21	21	4x100GbE node 21
22	4x100GbE node 22	22	4x100GbE node 22
23	4x100GbE node 23	23	4x100GbE node 23
24	4x100GbE node 24	24	4x100GbE node 24
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A	Cluster switch B	
1	1	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	
11	11	
12	12	
13	13	
14	14	
15	15	
16	16	
17	17	
18	18	
19	19	

Cluster switch A		Cluster switch B	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Cisco Nexus 92300YC cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	10/25 GbE node	1	10/25 GbE node
2	10/25 GbE node	2	10/25 GbE node
3	10/25 GbE node	3	10/25 GbE node
4	10/25 GbE node	4	10/25 GbE node
5	10/25 GbE node	5	10/25 GbE node
6	10/25 GbE node	6	10/25 GbE node
7	10/25 GbE node	7	10/25 GbE node

Cluster switch A		Cluster switch	В
8	10/25 GbE node	8	10/25 GbE node
9	10/25 GbE node	9	10/25 GbE node
10	10/25 GbE node	10	10/25 GbE node
11	10/25 GbE node	11	10/25 GbE node
12	10/25 GbE node	12	10/25 GbE node
13	10/25 GbE node	13	10/25 GbE node
14	10/25 GbE node	14	10/25 GbE node
15	10/25 GbE node	15	10/25 GbE node
16	10/25 GbE node	16	10/25 GbE node
17	10/25 GbE node	17	10/25 GbE node
18	10/25 GbE node	18	10/25 GbE node
19	10/25 GbE node	19	10/25 GbE node
20	10/25 GbE node	20	10/25 GbE node
21	10/25 GbE node	21	10/25 GbE node
22	10/25 GbE node	22	10/25 GbE node
23	10/25 GbE node	23	10/25 GbE node
24	10/25 GbE node	24	10/25 GbE node
25	10/25 GbE node	25	10/25 GbE node
26	10/25 GbE node	26	10/25 GbE node
27	10/25 GbE node	27	10/25 GbE node
28	10/25 GbE node	28	10/25 GbE node
29	10/25 GbE node	29	10/25 GbE node

Cluster switch A		Cluster switch E	3
30	10/25 GbE node	30	10/25 GbE node
31	10/25 GbE node	31	10/25 GbE node
32	10/25 GbE node	32	10/25 GbE node
33	10/25 GbE node	33	10/25 GbE node
34	10/25 GbE node	34	10/25 GbE node
35	10/25 GbE node	35	10/25 GbE node
36	10/25 GbE node	36	10/25 GbE node
37	10/25 GbE node	37	10/25 GbE node
38	10/25 GbE node	38	10/25 GbE node
39	10/25 GbE node	39	10/25 GbE node
40	10/25 GbE node	40	10/25 GbE node
41	10/25 GbE node	41	10/25 GbE node
42	10/25 GbE node	42	10/25 GbE node
43	10/25 GbE node	43	10/25 GbE node
44	10/25 GbE node	44	10/25 GbE node
45	10/25 GbE node	45	10/25 GbE node
46	10/25 GbE node	46	10/25 GbE node
47	10/25 GbE node	47	10/25 GbE node
48	10/25 GbE node	48	10/25 GbE node
49	40/100 GbE node	49	40/100 GbE node
50	40/100 GbE node	50	40/100 GbE node
51	40/100 GbE node	51	40/100 GbE node

Cluster switch A		Cluster switch B	
52	40/100 GbE node	52	40/100 GbE node
53	40/100 GbE node	53	40/100 GbE node
54	40/100 GbE node	54	40/100 GbE node
55	40/100 GbE node	55	40/100 GbE node
56	40/100 GbE node	56	40/100 GbE node
57	40/100 GbE node	57	40/100 GbE node
58	40/100 GbE node	58	40/100 GbE node
59	40/100 GbE node	59	40/100 GbE node
60	40/100 GbE node	60	40/100 GbE node
61	40/100 GbE node	61	40/100 GbE node
62	40/100 GbE node	62	40/100 GbE node
63	40/100 GbE node	63	40/100 GbE node
64	40/100 GbE node	64	40/100 GbE node
65	100 GbE ISL to switch B port 65	65	100 GbE ISL to switch A port 65
66	100 GbE ISL to switch B port 66	66	100 GbE ISL to switch A port 65

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	

3 3 4 4 5 5 6 6 7 7 8 8 9 9 10 10 11 11 12 12 13 13
5 5 6 6 7 7 8 8 9 9 10 10 11 11 12 12
6 6 7 7 8 8 9 9 10 10 11 11 12 12
7 7 8 8 9 9 10 10 11 11 12 12
8 8 9 9 10 10 11 11 12 12
9 9 10 10 11 11 12 12
10 10 11 11 12 12
11 11 12 12
12
13
14 14
15
16
17
18
19
20 20
21 21
22
23
24

Cluster switch A	Cluster switch B	
25	25	
26	26	
27	27	
28	28	
29	29	
30	30	
31	31	
32	32	
33	33	
34	34	
35	35	
36	36	
37	37	
38	38	
39	39	
40	40	
41	41	
42	42	
43	43	
44	44	
45	45	
46	46	

Cluster switch A		Cluster switch B	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL to switch B port 65	65	ISL to switch A port 65
66	ISL to switch B port 66	66	ISL to switch A port 66

Cisco Nexus 3232C cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling

worksheet by using the completed sample cabling worksheet as a guide. Each switch can be configured as a single 100GbE, 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G/100G node	1	4x10G/40G/100G node
2	4x10G/40G/100G node	2	4x10G/40G/100G node
3	4x10G/40G/100G node	3	4x10G/40G/100G node
4	4x10G/40G/100G node	4	4x10G/40G/100G node
5	4x10G/40G/100G node	5	4x10G/40G/100G node
6	4x10G/40G/100Gnode	6	4x10G/40G/100Gnode
7	4x10G/40G/100G node	7	4x10G/40G/100G node
8	4x10G/40G/100G node	8	4x10G/40G/100G node
9	4x10G/40G/100G node	9	4x10G/40G/100G node
10	4x10G/40G/100G node	10	4x10G/40G/100G node
11	4x10G/40G/100G node	11	4x10G/40G/100G node
12	4x10G/40G/100G node	12	4x10G/40G/100G node
13	4x10G/40G/100G node	13	4x10G/40G/100G node
14	4x10G/40G/100G node	14	4x10G/40G/100G node
15	4x10G/40G/100G node	15	4x10G/40G/100G node
16	4x10G/40G/100G node	16	4x10G/40G/100G node
17	4x10G/40G/100G node	17	4x10G/40G/100G node
18	4x10G/40G/100G node	18	4x10G/40G/100G node

Cluster switch A		Cluster switch B	
19	40G/100G node 19	19	40G/100G node 19
20	40G/100G node 20	20	40G/100G node 20
21	40G/100G node 21	21	40G/100G node 21
22	40G/100G node 22	22	40G/100G node 22
23	40G/100G node 23	23	40G/100G node 23
24	40G/100G node 24	24	40G/100G node 24
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	

Cluster switch A		Cluster switch B	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Cisco Nexus 3132Q-V cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide. Each switch can

be configured as a single 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G node	1	4x10G/40G node
2	4x10G/40G node	2	4x10G/40G node
3	4x10G/40G node	3	4x10G/40G node
ļ	4x10G/40G node	4	4x10G/40G node
5	4x10G/40G node	5	4x10G/40G node
3	4x10G/40G node	6	4x10G/40G node
7	4x10G/40G node	7	4x10G/40G node
3	4x10G/40G node	8	4x10G/40G node
9	4x10G/40G node	9	4x10G/40G node
10	4x10G/40G node	10	4x10G/40G node
11	4x10G/40G node	11	4x10G/40G node
12	4x10G/40G node	12	4x10G/40G node
13	4x10G/40G node	13	4x10G/40G node
14	4x10G/40G node	14	4x10G/40G node
15	4x10G/40G node	15	4x10G/40G node
16	4x10G/40G node	16	4x10G/40G node
17	4x10G/40G node	17	4x10G/40G node
18	4x10G/40G node	18	4x10G/40G node
19	40G node 19	19	40G node 19

Cluster switch A		Cluster switch B		
20	40G node 20	20	40G node 20	
21	40G node 21	21	40G node 21	
22	40G node 22	22	40G node 22	
23	40G node 23	23	40G node 23	
24	40G node 24	24	40G node 24	
25 through 30	Reserved	25 through 30	Reserved	
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31	
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32	

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B		
Switch port	Node/port usage	Switch port	Node/port usage	
1		1		
2		2		
3		3		
4		4		
5		5		
6		6		
7		7		
8		8		
9		9		

Cluster switch A		Cluster switch B		
10		10		
11		11		
12		12		
13		13		
14		14		
15		15		
16		16		
17		17		
18		18		
19		19		
20		20		
21		21		
22		22		
23		23		
24		24		
25 through 30	Reserved	25 through 30	Reserved	
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31	
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32	

Cisco Nexus 5596UP and 5596T cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

Some platforms support more than one 10GbE cluster port connection per cluster interconnect switch. To support additional cluster connections, you can use ports 25 through 40, as well as ports 49 through 80 when expansion modules are installed.

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	Node port 1	1	Node port 1
2	Node port 2	2	Node port 2
3	Node port 3	3	Node port 3
4	Node port 4	4	Node port 4
5	Node port 5	5	Node port 5
6	Node port 6	6	Node port 6
7	Node port 7	7	Node port 7
8	Node port 8	8	Node port 8
9	Node port 9	9	Node port 9
10	Node port 10	10	Node port 10
11	Node port 11	11	Node port 11
12	Node port 12	12	Node port 12
13	Node port 13	13	Node port 13
14	Node port 14	14	Node port 14
15	Node port 15	15	Node port 15
16	Node port 16	16	Node port 16
17	Node port 17	17	Node port 17
18	Node port 18	18	Node port 18

Cluster switch A		Cluster switch B		
19	Node port 19	19	Node port 19	
20	Node port 20	20	Node port 20	
21	Node port 21	21	Node port 21	
22	Node port 22	22	Node port 22	
23	Node port 23	23	Node port 23	
24	Node port 24	24	Node port 24	
25 through 40	Reserved	25 through 40	Reserved	
41	ISL to switch B port 41	41	ISL to switch A port 41	
42	ISL to switch B port 42	42	ISL to switch A port 42	
43	ISL to switch B port 43	43	ISL to switch A port 43	
44	ISL to switch B port 44	44	ISL to switch A port 44	
45	ISL to switch B port 45	45	ISL to switch A port 45	
46	ISL to switch B port 46	46	ISL to switch A port 46	
47	ISL to switch B port 47	47	ISL to switch A port 47	
48	ISL to switch B port 48	48	ISL to switch A port 48	

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.



Switch ports 1 through 24 function as 10 GbE ports. Switch ports 41 through 48 are reserved for Inter-Switch Links (ISLs).

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port Node/port usage	
1		1	

Cluster switch A	Cluster switch B	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	
11	11	
12	12	
13	13	
14	14	
15	15	
16	16	
17	17	
18	18	
19	19	
20	20	
21	21	
22	22	
23	23	

Cluster switch A		Cluster switch B		
24		24		
25 through 40	Reserved	25 through 40	Reserved	
41	ISL to switch B port 41	41	ISL to switch A port 41	
42	ISL to switch B port 42	42	ISL to switch A port 42	
43	ISL to switch B port 43	43	ISL to switch A port 43	
44	ISL to switch B port 44	44	ISL to switch A port 44	
45	ISL to switch B port 45	45	ISL to switch A port 45	
46	ISL to switch B port 46	46	ISL to switch A port 46	
47	ISL to switch B port 47	47	ISL to switch A port 47	
48	ISL to switch B port 48	48	ISL to switch A port 48	

Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 cluster switches

Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 cluster switches

The Cisco NX-OS software and reference configuration files (RCFs) must be installed on Cisco Nexus 9336C-FX2 cluster switches.

The following conditions must exist before you install the NX-OS software and Reference Configurations Files (RCFs) on the cluster switch:

- The cluster must be fully functioning (there should be no errors in the logs or similar issues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have a console connection to the switch, required when installing the RCF.
- You must have consulted the switch compatibility table on the Cisco Ethernet switch page for the supported ONTAP, NX-OS, and RCF versions.
- There can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on **Cisco Nexus 9000**

Series Switches.

Cisco Nexus 9000 Series Switches

· You must have the current RCF.



Before installing a new switch software version and RCFs, you must erase the switch settings and perform basic configuration. You must be connected to the switch using the serial console. This task resets the configuration of the management network.

The examples in this procedure use two nodes. These nodes use two 10GbE cluster interconnect ports e0a and e0b.

See the Hardware Universe to verify the correct cluster ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are cluster1-01 and cluster1-02.
- The cluster LIF names are cluster1-01_clus1 and cluster1-01_clus2 for cluster1-01 and cluster1-02_clus1 and cluster1-02 clus2 for cluster1-02.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=x h

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Change the privilege level to advanced, entering v when prompted to continue:

set -privilege advanced

The advanced prompt (*>) appears.

3. Display how many cluster interconnect interfaces are configured in each node for each cluster interconnect switch: network device-discovery show -protocol cdp

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
cluster1-0	2/cdp			
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-0	1/cdp			
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

- 4. Check the administrative or operational status of each cluster interface.
 - a. Display the network port attributes: network port show -ipspace Cluster

<pre>cluster1::*> network port show -ipspace Cluster</pre>							
Node: clu	ster1-02						
						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
Node: clu	ster1-01						
						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
4 entries	were display	ed.					

b. Display information about the LIFs: network interface show -vserver Cluster

<pre>cluster1::*> network interface show -vserver Cluster</pre>							
	Logical	Status	Network	Current			
Current Is							
Vserver	Interface	Admin/Oper	Address/Mask	Node			
Port Home	е						
Cluster							
	cluster1-01_clus1	up/up	169.254.209.69/16				
cluster1-01	e0a true						
	cluster1-01_clus2	up/up	169.254.49.125/16				
cluster1-01	e0b true						
	cluster1-02_clus1	up/up	169.254.47.194/16				
cluster1-02	e0a true						
	cluster1-02_clus2	up/up	169.254.19.183/16				
cluster1-02	e0b true						
4 entries we	ere displayed.						

 $[\]hbox{5. Ping the remote cluster LIFs: } \hbox{cluster ping-cluster -node node-name} \\$

```
cluster1::*> cluster ping-cluster -node cluster1-02
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01 clus1 169.254.209.69 cluster1-01
                                                         e0a
Cluster cluster1-01 clus2 169.254.49.125 cluster1-01
                                                         e0b
Cluster cluster1-02 clus1 169.254.47.194 cluster1-02
                                                         e0a
Cluster cluster1-02 clus2 169.254.19.183 cluster1-02
                                                         e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Verify that the auto-revert command is enabled on all cluster LIFs: network interface show -vserver Cluster -fields auto-revert

```
Cluster1::*> network interface show -vserver Cluster -fields auto-revert

Logical
Vserver Interface Auto-revert

Cluster

cluster1-01_clus1 true
cluster1-01_clus2 true
cluster1-02_clus1 true
cluster1-02_clus2 true
4 entries were displayed.
```

7. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system switch ethernet log setup-password and system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? \{y|n\}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

8. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 9336C-FX2 cluster switch.

Steps

1. Connect the cluster switch to the management network.

2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the NX-OS software and EPLD images to the Nexus 9336C-FX2 switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Verify the running version of the NX-OS software:

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
 BIOS compile time: 05/29/2020
 NXOS image file is: bootflash://nxos.9.3.4.bin
 NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]
Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FOC20291J6K
  Device name: cs2
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
Service:

plugin
Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. Install the NX-OS image.

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[############### 100% -- SUCCESS
Verifying image type.
[############### 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[############### 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[############### 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
                                                         9.3(5)
       nxos 9.3(4)
yes
       bios v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)
                   yes
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.
```

6. Verify the new version of NX-OS software after the switch has rebooted: show version

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and
```

```
otherwise stated, there is no warranty, express or implied, including
limited to warranties of merchantability and fitness for a particular
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 05.33
 NXOS: version 9.3(5)
 BIOS compile time: 09/08/2018
 NXOS image file is: bootflash:///nxos.9.3.5.bin
 NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FOC20291J6K
  Device name: cs2
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 277524 usecs after Mon Nov 2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

cs2# show version module 1 epld EPLD Device Version _____ MI FPGA 0x7 IO FPGA 0x17 0x2MI FPGA2 GEM FPGA 0x2GEM FPGA 0x2GEM FPGA 0x2GEM FPGA 0x2cs2# install epld bootflash:n9000-epld.9.3.5.img module 1 Compatibility check: Upgradable Impact Reason Module Type 1 SUP Yes disruptive Module Upgradable Retrieving EPLD versions.... Please wait. Images will be upgraded according to following table: Running-Version New-Version Upg-Module Type EPLD Required _____ 1 SUP MI FPGA 0x07 0x07 No 1 SUP IO FPGA 0x17 0x19 Yes 1 SUP MI FPGA2 0x02 0x02 No The above modules require upgrade. The switch will be reloaded at the end of the upgrade Do you want to continue (y/n) ? [n] y Proceeding to upgrade Modules. Starting Module 1 EPLD Upgrade Module 1: IO FPGA [Programming]: 100.00% (64 of 64 sectors) Module 1 EPLD upgrade is successful. Module Type Upgrade-Result _____ 1 SUP Success EPLDs upgraded. Module 1 EPLD upgrade is successful.

After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

cs2#	show version module 1 epld	
EPLD	Device	Version
MI	FPGA	0x7
	FPGA	0x19
	FPGA2	0x2
GEM	FPGA	0x2

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 9336C-FX2 switch for the first time. You can also use this procedure to upgrade your RCF version.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names arecluster1-01, cluster1-02, cluster1-03, and cluster1-04.
- The cluster LIF names are cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1, and cluster1-04_clus2.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches: network devicediscovery show

		Discovered Device (LLDP: ChassisID)	Interface	Platform
cluster1-0	_			_
C9336C	e0a	cs1	Ethernet1/7	N9K-
C9336C	e0d	0.5.7	Ethernet1/7	NOV-
C9336C	eoa	C32	Ecuerueci//	NJK
cluster1-0	2/cdp			
	_	cs1	Ethernet1/8	N9K-
C9336C				
	e0d	cs2	Ethernet1/8	N9K-
C9336C				
cluster1-0	_			
	e0a	cs1	Ethernet1/1/1	N9K-
C9336C	01	0	D.1 .1/1/1	31077
C9336C	e0b	cs2	Ethernet1/1/1	N9K-
cluster1-0	4/cdn			
01400011 0	_	cs1	Ethernet1/1/2	N9K-
C9336C				
	e0b	cs2	Ethernet1/1/2	N9K-
C9336C				

- 2. Check the administrative and operational status of each cluster port.
 - a. Verify that all the cluster ports are up with a healthy status: network port show -role cluster

Node: clu	ster1-02						
.vode. cra	02						
Ignore							
II a a l ± la						Speed (Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	МТП	Admin/Oper	Status
Status	1156466	Diodaodo	Domaii		1110	riamiri, oper	beacub
 e0a	 Cluster	Cluster		110	9000	auto/10000	n
coa healthy f		CIUSCCI		αр	3000	auco, 100000	S
_	Cluster	Cluster		up	9000	auto/100000)
healthy f	alse						
8 entries	were displa	yed.					
Node: clu	ster1-03						
Ignore	<u>:</u>						
						Speed(Mbps)	Health
Health							
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
		_				4	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healths
false	OT UD CCT	CIGOCCI		αр	3000	4400/10000	iicai cii ₋
Node: clu	ster1-04						
Ignore							
-						Speed (Mbps)	Health
Health	TD	D 1	D .	T ' 1	NATE TO	7.1.1.70	
Port Status	IPspace	Broadcast	Domain	Link	M.T.N	Admin/Oper	Status
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
	Cluster	Cluster		up	9000	auto/10000	health
<pre>false cluster1:</pre>	di S						

b. Verify that all the cluster interfaces (LIFs) are on the home port: network interface show -role

		Logical	Status	Network	Current
Cur	rent Is				
Vse	rver	Interface	Admin/Oper	Address/Mask	Node
Por	t Hom	e			
Clu	ster	ala+a1 01 ala1	/	160 254 2 4/22	~11
0 1	e0a	cluster1-01_clus1 true	սք/ սք	169.254.3.4/23	cluster1-
ΟŢ	eva	cluster1-01 clus2	מוו/מוו	169.254.3.5/23	cluster1-
01	e0d	true	αργαρ	103.231.3.3723	CIGDCCII
		cluster1-02 clus1	up/up	169.254.3.8/23	cluster1-
02	e0a	true			
		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-
02	e0d	true			
		cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-
03	e0a	true			
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-
03	e0b	true	,	1.60 054 1 6/00	
0.4	- 0 -	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-
04	e0a	true	/	160 254 1 7/22	alua+am1
04	e0b	cluster1-04_clus2 true	up/up	169.254.1.7/23	cluster1-
		ere displayed.			

C. Verify that the cluster displays information for both cluster switches: system cluster-switch show -is-monitoring-enabled-operational true

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch
                           Type
                                              Address
                                                               Model
cs1
                           cluster-network 10.233.205.90
                                                              N9K-
C9336C
     Serial Number: FOCXXXXXXGD
     Is Monitored: true
           Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(5)
   Version Source: CDP
cs2
                           cluster-network 10.233.205.91 N9K-
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
           Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
   Version Source: CDP
cluster1::*>
```

3. Disable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif \* -auto
-revert false
```

4. On cluster switch cs2, shut down the ports connected to the cluster ports of the nodes.

```
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
```

5. Verify that the cluster LIFs have migrated to the ports hosted on cluster switch cs1. This might take a few seconds.network interface show -role cluster

		Logical	Status	Network	Current
Current	Is				
Vserver		Interface	Admin/Oper	Address/Mask	Node
Port	Home	е			
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0a	true		,		
0	6 7	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0a	fals		,	1.60 054 0 0/00	
- 0 -	4	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0a	true		/	169.254.3.9/23	cluster1-02
e0a	fals	cluster1-02_clus2	up/up	169.234.3.9/23	Cluster1-02
eva	Iali	cluster1-03 clus1	11n / 11n	169.254.1.3/23	cluster1-03
e0a	true	-	ир/ир	107.234.1.3/23	Clustell 05
Coa	CIU	cluster1-03 clus2	ıın/ıın	169.254.1.1/23	cluster1-03
e0a	fals	_	αργαρ	103.201.1.1, 20	CIUDCCII 03
coa	141	cluster1-04 clus1	מנו/מנו	169.254.1.6/23	cluster1-04
e0a	true	_	αρ, α _Ρ	103,1201,110, 20	01000011 01
		cluster1-04 clus2	up/up	169.254.1.7/23	cluster1-04
e0a	fals	-	I . I		
		ere displayed.			

6. Verify that the cluster is healthy: cluster show

<pre>cluster1::*> cluster Node</pre>		Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displ	ayed.		
cluster1::*>			

7. Clean the configuration on switch cs2 and perform a basic setup.



When updating or applying a new RCF, you must erase the switch settings and perform basic configuration. You must be connected to the switch using the serial console to erase switch settings.

a. Clean the configuration. This step requires a console connection to the switch.

```
cs2# write erase Warning: This command will erase the startup-configuration. Do you wish to proceed anyway? (y/n) [n] y cs2# reload This command will reboot the system. (y/n)? [n] y cs2#
```

- b. Perform a basic setup of the switch.
- 8. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

This example shows TFTP being used to copy an RCF to the bootflash on switch cs2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

9. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

This example shows the RCF file Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt being installed on switch cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-configecho-commands
```

10. Examine the banner output from the show banner moted command. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

```
cs2# show banner motd
****************
* NetApp Reference Configuration File (RCF)
* Switch : Nexus N9K-C9336C-FX2
* Filename : Nexus 9336C RCF v1.6-Cluster-HA-Breakout.txt
* Date : 10-23-2020
* Version : v1.6
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int e1/1/1-4,
e1/2/1-4
, e1/3/1-4
* Ports 4-6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int e1/4/1-
4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
* Undo breakout commands and return interfaces to 40/100G configuration
in confi
q mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25q-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
******************
*****
```

11. Verify that the RCF file is the correct newer version: show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

The RCF banner

- The node and port settings
- Customizations
 The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.
- 12. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

13. Reboot switch cs2. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs2# reload This command will reboot the system. (y/n)? [n] y
```

- 14. Verify the health of cluster ports on the cluster.
 - a. Verify that e0d ports are up and healthy across all nodes in the cluster: network port show -role cluster

```
cluster1::*> network port show -role cluster
Node: cluster1-01
Ignore
                                             Speed (Mbps) Health
Health
Port
        IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a
       Cluster
                   Cluster
                                  up
                                        9000 auto/10000 healthy
false
e0b Cluster
                    Cluster
                                   up
                                        9000 auto/10000 healthy
false
Node: cluster1-02
Ignore
                                             Speed (Mbps) Health
```

Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	 Cluster	Cluster		un	9000	auto/10000	healthy
false	CIUSCCI	Clustel		ир	3000	auco/10000	neartny
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: clu	ster1-03						
Ignore							
Health						Speed (Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a	Cluster	Cluster		up	9000	auto/10000)
healthy f		Cl			0000	/10000	2
healthy f	Cluster Calse	Cluster		up	9000	auto/10000	J
Node: clu	ster1-04						
Ignore							
3						Speed(Mbps)	Health
Health	IPspace	Prondenst	Domain	Tink	Mmti	Admin/Onor	C+ 2+11C
Status	irspace	Bloadcast	Domain	TITILK	MIO	AdiiIII/Opei	status
e0a	Cluster	Cluster		up	9000	auto/10000)
healthy f	alse						
	Cluster	Cluster		up	9000	auto/100000)
healthy f 8 entries	aise were displaye	ed.					

b. Verify the switch health from the cluster (this might not show switch cs2, since LIFs are not homed on e0d).

cluster1-0	1/cdp				
	e0a	cs1		Ethernet1/7	N9K-
C9336C				,	
	e0d	cs2		Ethernet1/7	N9K-
C9336C	300				
cluster01-	-2/cdp				
014000101	e0a	cs1		Ethernet1/8	N9K-
C9336C	coa	001		Edicineer, 0	11311
033300	e0d	cs2		Ethernet1/8	N9K-
C9336C	coa	002		Helicilice1/ 0	NOIL
cluster01-	-3/cdn				
CIUSCCIOI	e0a	cs1		Ethernet1/1/1	N9K-
C9336C	eva	CSI		ECHETHECT/1/1	NOIN
093300	e0b	cs2		Ethernet1/1/1	N9K-
C9336C	600	CSZ		TCHETHECT/1/1	M 2 W -
	11/00				
cluster1-0	_	1		Ethomot1 /1 /0	NT O TZ
002260	e0a	cs1		Ethernet1/1/2	N9K-
C9336C	- O1	0		Ethernet1/1/2	NT O T #
	e0b	cs2		EThernet I/I//	N9K-
cluster1::	_	em cluster	-switch show -is-	monitoring-enable	
cluster1::	_	em cluster	-switch show -is- Type		
cluster1:: -operation Switch	_	em cluster	Туре	monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1	_	em cluster	Туре	monitoring-enable	d
cluster1:: -operation Switch cs1 C9336C	aal true		Type cluster-network	monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1 C9336C Seria	aal true	r: FOCXXXX	Type cluster-network	monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1 C9336C Seria	al true	r: FOCXXXX	Type cluster-network	monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1 C9336C Seria Is M	al true I Number Monitored Reason	r: FOCXXXX d: true n: None	Type 	Monitoring-enable Address 10.233.205.90	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M	al true I Number Monitored Reason	r: FOCXXXX d: true n: None	Type 	monitoring-enable Address	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M	al true I Number Monitored Reason	r: FOCXXXX d: true n: None n: Cisco N	Type 	Monitoring-enable Address 10.233.205.90	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version	al true I Number Monitored Reason	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type 	Monitoring-enable Address 10.233.205.90	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version	al true Al Number Monitored Reason Version	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type 	Monitoring-enable Address 10.233.205.90	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio	al true Al Number Monitored Reason Version	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating Sy	Monitoring-enable Address 10.233.205.90	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Version cs2	al true Al Number Monitored Reason Version	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating Sy	Address 10.233.205.90 Testem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Version cs2 C9336C	al true Al Number Monitored Reason Version on Source	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 Testem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Version cs2 C9336C Seria	al true Al Number Monitored Reason Version on Source	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 Testem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Version cs2 C9336C Seria	al true Al Number Monitored Reason Version on Source Al Number Monitored	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 Testem (NX-OS) Soft	d Mode NX9- ware,
-operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria Is M	al true Al Number Monitored Reason On Source Al Number Monitored Reason	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP r: FOCXXXX d: true n: None	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 stem (NX-OS) Soft	Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria Is M	al true Al Number Monitored Reason On Source Al Number Monitored Reason	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP r: FOCXXXX d: true n: None	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 Testem (NX-OS) Soft	Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Version cs2 C9336C Seria Is M Software	al true Al Number Monitored Reason On Source Al Number Monitored Reason	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP r: FOCXXXX d: true n: None n: Cisco N	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 stem (NX-OS) Soft	Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Version Cs2 C9336C Seria Is M Software Version	al true Al Number Monitored Reason On Source Al Number Monitored Reason	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating Sy cluster-network	Address 10.233.205.90 stem (NX-OS) Soft	Mode NX9- ware,

2 entries were displayed.



You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on VLAN0092. Port consistency restored. 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001. Inconsistent peer vlan. 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

15. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes.

The following example uses the interface example output from step 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

16. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds.

network interface show -role cluster

Cluster	1::">	> network interface			C
Current	Τα	Logical	Status	Network	Current
	_	Interface	Admin/Oper	Address/Mask	Node
Port			Admini/Oper	Address/Mask	Node
	_				
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	fals	se			
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true	е			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	fals				
0.1		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0d	true	-	/	1.00 054 1 2/02	1 1 00
e0b	fals	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
eub	Idl		up/up	169.254.1.1/23	cluster1-03
e0b	true	-	up/up	109.254.1.1/25	Clustell-03
000	CIU	cluster1-04 clus1	מוו/מוו	169.254.1.6/23	cluster1-04
e0b	fals	-	αρ/αρ	103.201.1.0,20	01450011 01
		cluster1-04 clus2	up/up	169.254.1.7/23	cluster1-04
e0b	true	_			
8 entri	es we	ere displayed.			

17. Verify that the cluster is healthy: cluster show

<pre>cluster1::*> clus</pre>	ster show		
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were di	isplayed.		
<pre>cluster1::*></pre>			

- 18. Repeat Steps 7 to 14 on switch cs1.
- 19. Enable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif \* -auto
-revert True
```

20. Reboot switch cs1. You do this to trigger the cluster LIFs to revert to their home ports. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs1# reload This command will reboot the system. (y/n)? [n] y
```

21. Verify that the switch ports connected to the cluster ports are up.

```
cs1# show interface brief \| grep up
Eth1/1/1
          1
                                                       10G(D)
                 eth access up
                                   none
Eth1/1/2 1 eth access up
                                                       10G(D)
                                   none
Eth1/7
           1
                eth trunk up
                                                      100G(D)
                                   none
Eth1/8
      1 eth trunk up
                                   none
                                                      100G(D)
--
```

22. Verify that the ISL between cs1 and cs2 is functional: show port-channel summary

23. Verify that the cluster LIFs have reverted to their home port: network interface show -role cluster

CIUDCCI	/	> network interface Logical	Status		Current
Current	Is				
Vserver		Interface	Admin/Oper	Address/Mask	Node
Port	Home	9			
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	true				
0.1		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true		/	160 254 2 0/22	-1+1 00
e0d	true	_	up/up	169.254.3.8/23	cluster1-02
Coa	CIUC	cluster1-02 clus2	מנו/מנו	169.254.3.9/23	cluster1-02
e0d	true	-			
		cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0b	true	е			
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	true		,		
0.1		cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	true	e cluster1-04 clus2	11D/11D	169.254.1.7/23	cluster1-04
e0b	true	-	αρ/ αρ	107.407.1.1/40	CIUSCEII-04
		ere displayed.			

24. Verify that the cluster is healthy: ${\tt cluster}\ {\tt show}$

cluster1::*> cluster	show		
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were disp	ayed.		
cluster1::*>			

25. Ping the remote cluster interfaces to verify connectivity: cluster ping-cluster -node local

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03 clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03 clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04 clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04 clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01 clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01 clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02 clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02 clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
. . . . . . . . . . . .
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
   Local 169.254.1.3 to Remote 169.254.1.7
   Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
   Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
   Local 169.254.1.1 to Remote 169.254.1.6
   Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Migrate from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

Migrate from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

You must be aware of certain configuration information, port connections and cabling

requirements when you are replacing some older Cisco Nexus cluster switches with Cisco Nexus 9336C-FX2 cluster switches.

- The following cluster switches are supported:
 - Nexus 9336C-FX2
 - Nexus 92300YC
 - Nexus 5596UP
 - Nexus 3232C
 - Nexus 3132Q-V
- See the Hardware Universe for full details of supported ports and their configurations.
- You have configured some of the ports on Nexus 9336C-FX2 switches to run at 10 GbE or 40 GbE.
- You have planned, migrated, and documented 10 GbE and 40 GbE connectivity from nodes to Nexus 9336C-FX2 cluster switches.
- The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page.

How to migrate from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

You can migrate nondisruptively older Cisco cluster switches for an ONTAP cluster to Cisco Nexus 9336C-FX2 cluster network switches.

- The existing cluster must be properly set up and functioning.
- All cluster ports must be in the up state to ensure nondisruptive operations.
- The Nexus 9336C-FX2 cluster switches must be configured and operating under the proper version of NX-OS installed and reference configuration file (RCF) applied.
- The existing cluster network configuration must have the following:
 - A redundant and fully functional NetApp cluster using both older Cisco switches.
 - · Management connectivity and console access to both the older Cisco switches and the new switches.
 - All cluster LIFs in the up state with the cluster LIfs are on their home ports.
 - ISL ports enabled and cabled between the older Cisco switches and between the new switches.

The examples in this procedure use the following switch and node nomenclature:

- The existing Cisco Nexus 5596UP cluster switches are c1 and c2.
- The new Nexus 9336C-FX2 cluster switches are cs1 and cs2.
- The nodes are node1 and node2.
- The cluster LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- Switch c2 is replaced by switch cs2 first and then switch c1 is replaced by switch cs1.
 - A temporary ISL is built on cs2 connecting c2 to cs2.
 - Cabling between the nodes and c2 are then disconnected from c2 and reconnected to cs2.
 - Cabling between the nodes and c1 are then disconnected from c1 and reconnected to cs1.
 - The temporary ISL between c2 and cs2 is then removed.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Change the privilege level to advanced, entering **y** when prompted to continue: set -privilege advanced

The advanced prompt (*>) appears.

3. Verify that auto-revert is enabled on all cluster LIFs: network interface show -vserver Cluster -fields auto-revert

```
cluster1::*> network interface show -vserver Cluster -fields auto-revert

Logical
Vserver Interface Auto-revert

Cluster

node1_clus1 true
node1_clus2 true
node2_clus1 true
node2_clus1 true
node2_clus2 true
4 entries were displayed.
```

4. Determine the administrative or operational status for each cluster interface:

Each port should display up for Link and healthy for Health Status.

a. Display the network port attributes: network port show -ipspace Cluster

<pre>cluster1::*> network port show -ipspace Cluster</pre>									
Node: node1									
Ignore						Speed(Mbps)	Hoalth		
Health						speed (Mpps)	пеатсп		
Status	IPspace					_	Status		
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy		
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy		
Node: nod	de2								
_						Speed(Mbps)	Health		
Status	IPspace					_	Status		
	Cluster	Cluster		up	9000	auto/10000	healthy		
	Cluster	Cluster		up	9000	auto/10000	healthy		
4 entries	s were displa	yed.							

b. Display information about the logical interfaces and their designated home nodes: network interface show -vserver Cluster

Each LIF should display up/up for Status Admin/Oper and true for Is Home.

cluster1::*> network interface show -vserver Cluster								
		Logical	Status	Network	Current			
Current								
Vserver		Interface	Admin/Oper	Address/Mask	Node			
Port	Home	e						
		_						
Cluster								
		node1_clus1	up/up	169.254.209.69/16	node1			
e0a	tru							
		node1_clus2	up/up	169.254.49.125/16	node1			
e0b	tru	е						
		node2_clus1	up/up	169.254.47.194/16	node2			
e0a	tru	e						
		node2_clus2	up/up	169.254.19.183/16	node2			
e0b	tru	е						
4 entrie	es we	ere displayed						

5. The cluster ports on each node are connected to existing cluster switches in the following way (from the nodes' perspective) using the command: network device-discovery show -protocol cdp

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node1	/cdp			
	e0a	c1	0/1	N5K-
C5596UP				
	e0b	c2	0/1	N5K-
C5596UP				
node2	/cdp			
	e0a	c1	0/2	N5K-
C5596UP				
	e0b	c2	0/2	N5K-
C5596UP				

6. The cluster ports and switches are connected in the following way (from the switches' perspective) using the command: show cdp neighbors

```
c1# show cdp neighbors
```

V -	Router, T - Ti Switch, H - Ho VoIP-Phone, D Supports-STP-I	ost, I - - Remot	- IGMP, r - 1	Repeater,
Device-ID	Local Intrfce	Hldtme	Capability	Platform
Port ID node1	Eth1/1	124	Н	FAS2750
e0a node2 e0a	Eth1/2	124	Н	FAS2750
c2 Eth1/41	Eth1/41	179	S I s	N5K-C5596UP
c2 Eth1/42	Eth1/42	175	S I s	N5K-C5596UP
c2 Eth1/43	Eth1/43	179	SIs	N5K-C5596UP
c2 Eth1/44	Eth1/44	175	SIs	N5K-C5596UP
c2 Eth1/45	Eth1/45	179	SIs	N5K-C5596UP
c2 Eth1/46	Eth1/46	179	SIs	N5K-C5596UP
c2 Eth1/47	Eth1/47	175	SIs	N5K-C5596UP
c2 Eth1/48	Eth1/48	179	SIs	N5K-C5596UP
Total entries display	zed: 10			
c2# show cdp neighbor	`s			
V -	Router, T - Ti Switch, H - Ho VoIP-Phone, D Supports-STP-I	ost, I - - Remot	- IGMP, r - 1	Repeater,
Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1	Eth1/1	124	Н	FAS2750
node2 e0b	Eth1/2	124	Н	FAS2750
c1 Eth1/41	Eth1/41	175	SIs	N5K-C5596UP

c1	Eth1/42	175	SIS	N5K-C5596UP
Eth1/42				
c1	Eth1/43	175	SIS	N5K-C5596UP
Eth1/43				
C1	Eth1/44	175	SIS	N5K-C5596UP
Eth1/44 c1	Eth1/45	175	SIs	N5K-C5596UP
Eth1/45	ECIII/45	175	5 1 5	N3K-C33900P
c1	Eth1/46	175	SIs	N5K-C5596UP
Eth1/46				
c1	Eth1/47	176	SIs	N5K-C5596UP
Eth1/47				
c1	Eth1/48	176	S I s	N5K-C5596UP
Eth1/48				

7. Ensure that the cluster network has full connectivity using the command: cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
                                             e0a
Cluster node1 clus2 169.254.49.125 node1
                                             e0b
Cluster node2 clus1 169.254.47.194 node2
                                             e0a
Cluster node2 clus2 169.254.19.183 node2
                                             e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

8. Configure a temporary ISL on cs1 on ports e1/33-34, between c1 and cs1.

The following example shows how the new ISL is configured on c1 and cs1:

```
cs2# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config) # interface e1/33-34
cs2(config-if-range)# description temporary ISL between Nexus 5596UP and
Nexus 9336C
cs2(config-if-range) # no lldp transmit
cs2(config-if-range) # no lldp receive
cs2(config-if-range)# switchport mode trunk
cs2(config-if-range)# no spanning-tree bpduguard enable
cs2(config-if-range) # channel-group 101 mode active
cs2(config-if-range)# exit
cs2(config) # interface port-channel 101
cs2(config-if)# switchport mode trunk
cs2(config-if) # spanning-tree port type network
cs2(config-if)# exit
cs2(config)# exit
```

- 9. Remove ISL cables from ports e1/33-34 from c2 and connect the cables to ports e1/33-34 on cs2.
- 10. Verify that the ISL ports and port-channel are operational connecting c2 and cs2: show port-channel summary

The following example shows the Cisco show port-channel summary command being used to verify the ISL ports are operational on c2 and cs2:

```
c2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/41(P) Eth1/42(P)
Eth1/43(P)
                                Eth1/44(P) Eth1/45(P)
Eth1/46(P)
                                 Eth1/47(P) Eth1/48(P)
cs2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/35(P) Eth1/36(P)
101 Po101(SU) Eth LACP
                                Eth1/41(P) Eth1/42(P)
Eth1/43(P)
                                Eth1/44(P) Eth1/45(P)
Eth1/46(P)
                                 Eth1/47(P) Eth1/48(P)
```

11. For node1, disconnect the cable from e1/1 on c2, and then connect the cable to e1/1 on cs2, using

- appropriate cabling supported by Nexus 9336C-FX2.
- 12. For node2, disconnect the cable from e1/2 on c2, and then connect the cable to e1/2 on cs2, using appropriate cabling supported by Nexus 9336C-FX2.
- 13. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective: network device-discovery show -protocol cdp

cluster1::*> network device-discovery show -protocol cdp								
		Discovered Device (LLDP: ChassisID)	Interface	Platform				
node1	/cdp							
	e0a	c1	0/1	N5K-				
C5596UP								
	e0b	cs2	0/1	N9K-				
C9336C								
	/ = =]==							
node2	/cdp	-1	0 / 0	NT E TZ				
C5596UP	e0a	CI	0/2	N5K-				
C33300F	e0b	cs2	0/2	N9K-				
C9336C	COD	002	J, 2	1,31				

- 14. For node1, disconnect the cable from e1/1 on c1, and then connect the cable to e1/1 on cs1, using appropriate cabling supported by Nexus 9336C-FX2.
- 15. For node2, disconnect the cable from e1/2 on c1, and then connect the cable to e1/2 on cs1, using appropriate cabling supported by Nexus 9336C-FX2.
- 16. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective: network device-discovery show -protocol cdp

cluster1::	<pre>cluster1::*> network device-discovery show -protocol cdp</pre>								
Node/	Local	Discovered							
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform					
node1	/cdp								
	e0a	cs1	0/1	N9K-					
C9336C									
	e0b	cs2	0/1	N9K-					
C9336C									
node2	/cdp								
	e0a	cs1	0/2	N9K-					
C9336C									
	e0b	cs2	0/2	N9K-					
C9336C									

17. Delete the temporary ISL between cs1 and c1.

```
csl(config)# no interface port-channel 101
csl(config)# interface e1/33-34
csl(config-if-range)# 1ldp transmit
csl(config-if-range)# 1ldp receive
csl(config-if-range)# no switchport mode trunk
csl(config-if-range)# no channel-group
csl(config-if-range)# description 10GbE Node Port
csl(config-if-range)# spanning-tree bpduguard enable
csl(config-if-range)# exit
csl(config)# exit
```

18. Verify the final configuration of the cluster: network port show -ipspace Cluster

Each port should display up for Link and healthy for Health Status.

```
Cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore

Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
```

	Cluster	Cluster		up	9000	auto/10000	healthy
false	Cl	Q1a.t			0000		h = = 1 + 1
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
raise							
Node: node	2						
Ignore							
Health						Speed (Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status	110000	210000000	201101211		1110	110111111, OP 01	
	Cl	Q1a.t			0000		h = = 1 + 1
eUa false	Cluster	Cluster		up	9000	auto/10000	neartny
	Cluster	Cluster		up	9000	auto/10000	healthv
				T-		2, 2, 2, 3, 3, 0	1
4 entries	were display **> network i		ow -vs	erver	Clus	ter	
4 entries	**> network i Logical				Clus	ter Current	
4 entries cluster1::	*> network i Logical	nterface sh Status	Netwo:	rk		Current	Port
4 entries cluster1:: Current Is	*> network i Logical	nterface sh	Netwo:	rk		Current	Port
4 entries cluster1:: Current Is	*> network i Logical	nterface sh Status	Netwo:	rk		Current	Por†
4 entries cluster1:: Current Is Vserver Home	Logical Interface	nterface sh Status Admin/Oper	Netwo:	rk ss/Mas	sk 	Current Node	
4 entries cluster1:: Current Is Vserver Home Cluster	Logical Interface	nterface sh Status	Netwo:	rk ss/Mas	sk 	Current Node	Port e0a
	Logical Interface node1_clus	nterface sh Status Admin/Oper	Netwo: Addre: 169.2	rk ss/Mas	sk 9.69/1	Current Node	
4 entries cluster1:: Current Is Vserver Home Cluster true	Logical Interface node1_clus	nterface sh Status Admin/Oper 1 up/up 2 up/up	Netwo: Addre: 169.25	rk ss/Mas 54.209	sk 9.69/1	Current Node 16 node1 16 node1	 e0a
4 entries cluster1:: Current Is Vserver Home Cluster true true	Logical Interface node1_clus	nterface sh Status Admin/Oper 1 up/up	Netwo: Addre: 169.25	rk ss/Mas 54.209	sk 9.69/1	Current Node 16 node1 16 node1	 e0a
4 entries cluster1:: Current Is Vserver Home Cluster true	Logical Interface node1_clus node2_clus	nterface sh Status Admin/Oper 1 up/up 2 up/up 1 up/up	Netwo: Addre: 169.2: 169.2: 169.2:	rk ss/Mas 54.209 54.49	sk 9.69/: .125/:	Current Node 16 node1 16 node1 16 node2	e0a e0b e0a
4 entries cluster1:: Current Is Vserver Home Cluster true true	Logical Interface node1_clus node2_clus	nterface sh Status Admin/Oper 1 up/up 2 up/up	Netwo: Addre: 169.2: 169.2: 169.2:	rk ss/Mas 54.209 54.49	sk 9.69/: .125/:	Current Node 16 node1 16 node1	e0a e0b
4 entries cluster1:: Current Is Vserver Home Cluster true true true	Logical Interface node1_clus node2_clus	nterface sh Status Admin/Oper 1 up/up 2 up/up 1 up/up 2 up/up 2 up/up	Netwo: Addre: 169.2: 169.2: 169.2:	rk ss/Mas 54.209 54.49	sk 9.69/: .125/:	Current Node 16 node1 16 node1 16 node2	e0a e0b e0a

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	0/2	N9K-
C9336C				
	e0b	cs2	0/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C9336C				
	e0b	cs2	0/1	N9K-
C9336C				

⁴ entries were displayed.

19. Verify that both nodes each have one connection to each switch: show cdp neighbors

The following example shows the appropriate results for both switches:

cs1# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Port ΙD node1 Eth1/1 124 Η FAS2750 e0a Eth1/2 e0a node2 124 FAS2750 Eth1/35 cs2 179 RSIs N9K-C9336C Eth1/35 cs2 Eth1/36 179 R S I s N9K-C9336C Eth1/36 cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Port TD Eth1/1 e0b node1 124 Н FAS2750 node2 e0b Eth1/2 124 FAS2750 Η cs1 Eth1/35 179 RSIS N9K-C9336C Eth1/35 cs1 Eth1/36 179 R S I S N9K-C9336C Eth1/36 Total entries displayed: 4

^{20.} Ensure that the cluster network has full connectivity: cluster ping-cluster -node node-name

```
cluster1::*> set -priv advanced
Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? \{y|n\}: y
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
Cluster node1 clus2 169.254.49.125 node1
                                               e0b
Cluster node2 clus1 169.254.47.194 node2
                                               e0a
Cluster node2 clus2 169.254.19.183 node2
                                               e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
cluster1::*> set -privilege admin
cluster1::*>
```

21. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the following two commands: system switch ethernet log setup-password and system switch ethernet log enable-collection

Enter: system switch ethernet log setup-password

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? \{y|n\}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Followed by: system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



If any of these commands return an error, contact NetApp support.

22. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system cluster-switch log setup-password and system cluster-switch log enable-collection

Enter: system cluster-switch log setup-password

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Followed by: system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



If any of these commands return an error, contact NetApp support.

23. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Migrate to a two-node switched cluster with Cisco Nexus 9336C-FX2 cluster switches

Migrate to a two-node switched cluster with Cisco Nexus 9336C-FX2 cluster switches

You must be aware of certain configuration information, port connections, and cabling requirements when you migrate a two-node switchless cluster, non-disruptively, to a cluster with Cisco Nexus 9336C-FX2 cluster switches. The procedure you use depends on whether you have two dedicated cluster-network ports on each controller or a single cluster port on each controller. The process documented works for all nodes using optical or Twinax ports but is not supported on this switch if nodes are using onboard 10Gb BASE-T RJ45 ports for the cluster-network ports.

Most systems require two dedicated cluster-network ports on each controller. See Cisco Ethernet switches

How to migrate to a switched NetApp cluster environment with Cisco Nexus 9336C-FX2 cluster switches

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using Cisco Nexus 9336C-FX2 switches to enable you to scale beyond two nodes in the cluster.

Two-node switchless configuration:

- The two-node switchless configuration must be properly set up and functioning.
- The nodes must be running ONTAP 9.8 and later.
- All cluster ports must be in the up state.
- All cluster logical interfaces (LIFs) must be in the up state and on their home ports.

Cisco Nexus 9336C-FX2 switch configuration:

- Both switches must have management network connectivity.
- There must be console access to the cluster switches.
- Nexus 9336C-FX2 node-to-node switch and switch-to-switch connections must use Twinax or fiber cables.

The Hardware Universe - Switches contains more information about cabling.

Hardware Universe - Switches

- Inter-Switch Link (ISL) cables must be connected to ports 1/35 and 1/36 on both 9336C-FX2 switches.
- Initial customization of both the 9336C-FX2 switches must be completed. So that the:
 - 9336C-FX2 switches are running the latest version of software
 - Reference Configuration Files (RCFs) have been applied to the switches
 Any site customization, such as SMTP, SNMP, and SSH must be configured on the new switches.

The examples in this procedure use the following cluster switch and node nomenclature:

- The names of the 9336C-FX2 switches are cs1 and cs2.
- The names of the cluster SVMs are node1 and node2.
- The names of the LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- The cluster1::*> prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e0a and e0b.

The Hardware Universe contains the latest information about the actual cluster ports for your platforms.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

 Change the privilege level to advanced, entering y when prompted to continue: set -privilege advanced

The advanced prompt (*>) appears.

3. Disable all node-facing ports (not ISL ports) on both the new cluster switches cs1 and cs2.

You must not disable the ISL ports.

The following example shows that node-facing ports 1 through 34 are disabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e/1-34
cs1(config-if-range)# shutdown
```

4. Verify that the ISL and the physical ports on the ISL between the two 9336C-FX2 switches cs1 and cs2 are up on ports 1/35 and 1/36: show port-channel summary

The following example shows that the ISL ports are up on switch cs1:

The following example shows that the ISL ports are up on switch cs2:

5. Display the list of neighboring devices: show cdp neighbors

This command provides information about the devices that are connected to the system.

The following example lists the neighboring devices on switch cs1:

```
cs1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                 Local Intrfce Hldtme Capability Platform
                                                               Port
ΙD
                 Eth1/35
cs2
                               175 RSIS
                                                 N9K-C9336C
Eth1/35
                 Eth1/36
cs2
                               175 RSIS
                                                 N9K-C9336C
Eth1/36
Total entries displayed: 2
```

The following example lists the neighboring devices on switch cs2:

```
cs2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                 Local Intrfce Hldtme Capability Platform
                                                               Port
ID
cs1
                 Eth1/35
                               177 R S I s N9K-C9336C
Eth1/35
cs1
                Eth1/36
                               177 R S I S N9K-C9336C
             )
Eth1/36
Total entries displayed: 2
```

6. Verify that all cluster ports are up: network port show -ipspace Cluster

Each port should display up for Link and healthy for Health Status.

cluster1:	:*> network p	ort show -i	pspace	Clust	ter		
Node: node	e1						
Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	
e0a e0b	Cluster Cluster	Cluster Cluster		up up	9000		-
Node: node	e2						
Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	
e0a e0b	Cluster Cluster	Cluster Cluster		up up	9000		_
4 entries	were display	ed.					

7. Verify that all cluster LIFs are up and operational: network interface show -vserver Cluster Each cluster LIF should display true for Is Home and have a Status Admin/Oper of up/up

cluster1::*	> network i	nterface sh	ow -vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	node1_clus	l up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	2 up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus	l up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	2 up/up	169.254.19.183/16	node2	e0b
true					
4 entries we	ere displaye	ed.			

8. Verify that auto-revert is enabled on all cluster LIFs: network interface show -vserver Cluster

9. Disconnect the cable from cluster port e0a on node1, and then connect e0a to port 1 on cluster switch cs1, using the appropriate cabling supported by the 9336C-FX2 switches.

The Hardware Universe - Switches contains more information about cabling.

Hardware Universe - Switches

- 10. Disconnect the cable from cluster port e0a on node2, and then connect e0a to port 2 on cluster switch cs1, using the appropriate cabling supported by the 9336C-FX2 switches.
- 11. Enable all node-facing ports on cluster switch cs1.

The following example shows that ports 1/1 through 1/34 are enabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# no shutdown
```

12. Verify that all cluster LIFs are up, operational, and display as true for Is Home: network interface show -vserver Cluster

The following example shows that all of the LIFs are up on node1 and node2 and that Is Home results are true:

cluster1	::*> network	interface sl	now -vserver Cluste	r	
	Logical	Status	Network	Current	Current
Is					
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true		,			
.	node1_clus2	up/up	169.254.49.125/16	nodel	e0b
true	node2 clus1	11n/11n	169.254.47.194/16	node?	e0a
true	110002_01051	αργαρ	103.231.17.131/10	110002	Coa
0200	node2 clus2	up/up	169.254.19.183/16	node2	e0b
true	<u> </u>				
4 entrie	s were displa	yed.			

13. Display information about the status of the nodes in the cluster: cluster show

The following example displays information about the health and eligibility of the nodes in the cluster:

- 14. Disconnect the cable from cluster port e0b on node1, and then connect e0b to port 1 on cluster switch cs2, using the appropriate cabling supported by the 9336C-FX2 switches.
- 15. Disconnect the cable from cluster port e0b on node2, and then connect e0b to port 2 on cluster switch cs2, using the appropriate cabling supported by the 9336C-FX2 switches.
- 16. Enable all node-facing ports on cluster switch cs2.

The following example shows that ports 1/1 through 1/34 are enabled on switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-34
cs2(config-if-range)# no shutdown
```

17. Verify that all cluster ports are up: network port show -ipspace Cluster

The following example shows that all of the cluster ports are up on node1 and node2:

```
cluster1::*> network port show -ipspace Cluster
Node: node1
Ignore
                                         Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster Cluster up 9000 auto/10000 healthy
false
      Cluster Cluster up 9000 auto/10000 healthy
e0b
false
Node: node2
Ignore
                                         Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
e0a Cluster Cluster up 9000 auto/10000 healthy
false
      Cluster Cluster up 9000 auto/10000 healthy
e0b
false
4 entries were displayed.
```

18. Verify that all interfaces display true for Is Home: network interface show -vserver Cluster



This might take several minutes to complete.

The following example shows that all LIFs are up on node1 and node2 and that Is Home results are true:

	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster		,			
	node1_clus1	up/up	169.254.209.69/16	nodel	e0a
true	1 1 1 0	,	160 054 40 105/16	. 1	0.1
.	node1_clus2	up/up	169.254.49.125/16	nodel	e0b
true		/	100 054 47 104/10		-0-
+ 2011.0	nodez_clusi	up/up	169.254.47.194/16	nodez	e0a
true	nodol alual	/	160 254 10 102/16	2000	o O b
true	nodez_crusz	up/up	169.254.19.183/16	nouez	e0b
CIUE					

19. Verify that both nodes each have one connection to each switch: show cdp neighbors

The following example shows the appropriate results for both switches:

```
(cs1) # show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                                  Port
ID
                  Eth1/1
node1
                                 133
                                        Н
                                                    FAS2980
                                                                  e0a
node2
                  Eth1/2
                                                    FAS2980
                                                                  e0a
                                 133
                  Eth1/35
                                                    N9K-C9336C
cs2
                                 175
                                        RSIs
Eth1/35
cs2
                  Eth1/36
                                 175
                                       RSIs
                                                    N9K-C9336C
Eth1/36
Total entries displayed: 4
(cs2) # show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                                  Port
ID
node1
                                                                  e0b
                  Eth1/1
                                 133
                                        Η
                                                    FAS2980
node2
                  Eth1/2
                                 133
                                                    FAS2980
                                                                  e0b
                                        Η
cs1
                  Eth1/35
                                 175
                                        RSIs
                                                    N9K-C9336C
Eth1/35
cs1
                  Eth1/36
                                 175 RSIS
                                                    N9K-C9336C
Eth1/36
Total entries displayed: 4
```

^{20.} Display information about the discovered network devices in your cluster: network device-discovery show -protocol cdp

		Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	0/2	N9K-
C9336C				
	e0b	cs2	0/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C9336C				
	e0b	cs2	0/1	N9K-
C9336C				

21. Verify that the settings are disabled: network options switchless-cluster show



It might take several minutes for the command to complete. Wait for the '3 minute lifetime to expire' announcement.

The false output in the following example shows that the configuration settings are disabled:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

22. Verify the status of the node members in the cluster: cluster show

The following example shows information about the health and eligibility of the nodes in the cluster:

23. Ensure that the cluster network has full connectivity: cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e0a
Cluster node1 clus2 169.254.49.125 node1 e0b
Cluster node2 clus1 169.254.47.194 node2 e0a
Cluster node2 clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

- 24. Change the privilege level back to admin: set -privilege admin
- 25. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system switch ethernet log setup-password and system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? \{y|n\}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

26. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? \{y|n\}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

27. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Configure a Cisco Nexus 9336C-FX2 cluster switch

Configure a Cisco Nexus 9336C-FX2 cluster switch

You can configure a new Nexus 9336C-FX2 switch by completing the steps detailed in

this chapter.

Installing the Nexus 9336C-FX2 switch on systems running ONTAP 9.8 and later, starts with setting up an IP address and configuration to allow the switch to communicate through the management interface. You can then install the NX-OS software and reference configuration file (RCF). This procedure is intended for preparing the Nexus 9336C-FX2 switch before controllers are added.

The examples in this procedure use the following switch and node nomenclature:

- The Nexus 9336C-FX2 switch names are cs1 and cs2.
- The example used in this procedure starts the upgrade on the second switch, *cs2*.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The IPspace name is Cluster.
- The cluster1::*> prompt indicates the name of the cluster.
- The cluster ports on each node are named e0a and e0b.

See the Hardware Universe for the actual cluster ports supported on your platform.

- The node connections supported for the Nexus 9336C-FX2 switches are ports 1/1 through 1/34.
- The Inter-Switch Links (ISLs) supported for the Nexus 9336C-FX2 switches are ports 1/35 and 1/36.
- The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.

Initial installation of the Nexus 9336C-FX2 cluster switch

You can use this procedure to perform the initial installation of the Cisco Nexus 9336C-FX2 switch.

You can download the applicable NetApp Cisco NX-OS software for your switches from the NetApp Support Site at mysupport.netapp.com.

NX-OS is a network operating system for the Nexus series of Ethernet switches and MDS series of Fibre Channel (FC) storage area network switches provided by Cisco Systems.

This procedure provides a summary of the process to install your switches and get them running.

Steps

- 1. Connect the serial port to the host or serial port of your choice.
- 2. Connect the management port (on the non-port side of the switch) to the same network where your SFTP server is located.
- 3. At the console, set the host side serial settings:
 - · 9600 baud
 - 8 data bits
 - 1 stop bit
 - · parity: none
 - · flow control: none
- 4. Booting for the first time or rebooting after erasing the running configuration, the Nexus 9336C-FX2 switch

loops in a boot cycle. Interrupt this cycle by typing **yes** to abort Power on Auto Provisioning. You are then presented with the System Admin Account setup:

```
$ VDC-1 %$ %POAP-2-POAP_INFO: - Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic configuration, no - continue with Power On Auto Provisioning] (yes/skip/no)[no]: yes Disabling POAP......Disabling POAP 2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please wait... (This may take 5-15 minutes)
```

5. Type **y** to enforce secure password standard:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Enter and confirm the password for user admin:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Enter the Basic System Configuration dialog:

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 Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 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.

Would you like to enter the basic configuration dialog (yes/no):

8. Create another login account:

```
Create another login account (yes/no) [n]:
```

9. Configure read-only and read-write SNMP community strings:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

10. Configure the cluster switch name:

```
Enter the switch name : cs2
```

11. Configure the out-of-band management interface:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address: 172.22.133.216

Mgmt0 IPv4 netmask: 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway: 172.22.128.1
```

12. Configure advanced IP options:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Configure Telnet services:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Configure SSH services and SSH keys:

```
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]: 2048
```

15. Configure other settings:

```
Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L2]: L2

Configure default switchport interface state (shut/noshut) [noshut]: noshut

Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Confirm switch information and save the configuration:

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

Use this configuration and save it? (yes/no) [y]: y

[################################# 100%

Copy complete, now saving to disk (please wait)...

Copy complete.
```

17. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system switch ethernet log setup-password and system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? \{y|n\}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

18. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 9336C-FX2 cluster switch.

Steps

1. Connect the cluster switch to the management network.

2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the NX-OS software and EPLD images to the Nexus 9336C-FX2 switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
```

4. Verify the running version of the NX-OS software:

cs2# show version Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac Copyright (C) 2002-2020, Cisco and/or its affiliates. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and unless otherwise stated, there is no warranty, express or implied, including limited to warranties of merchantability and fitness for a particular purpose. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or GNU General Public License (GPL) version 3.0 or the GNU Lesser General Public License (LGPL) Version 2.1 or Lesser General Public License (LGPL) Version 2.0. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://opensource.org/licenses/gpl-3.0.html and http://www.opensource.org/licenses/lgpl-2.1.php and http://www.gnu.org/licenses/old-licenses/library.txt. Software BIOS: version 08.38 NXOS: version 9.3(4) BIOS compile time: 05/29/2020 NXOS image file is: bootflash://nxos.9.3.4.bin NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31] Hardware cisco Nexus9000 C9336C-FX2 Chassis Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory. Processor Board ID FOC20291J6K Device name: cs2 bootflash: 53298520 kB Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s) Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020 Reason: Reset Requested by CLI command reload System version: 9.3(4) Service:

```
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

5. Install the NX-OS image.

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[############### 100% -- SUCCESS
Verifying image type.
[############### 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[############### 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[############### 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
_____
_____
                                                   9.3(5)
 1 nxos 9.3(4)
yes
       bios v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)
                  yes
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.
```

6. Verify the new version of NX-OS software after the switch has rebooted: show version

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and unless otherwise stated, there is no warranty, express or implied, including
```

```
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 05.33
 NXOS: version 9.3(5)
 BIOS compile time: 09/08/2018
 NXOS image file is: bootflash://nxos.9.3.5.bin
 NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
 Processor Board ID FOC20291J6K
 Device name: cs2
 bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 277524 usecs after Mon Nov 2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:
plugin
 Core Plugin, Ethernet Plugin
Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

cs2# show v	ersion module	1 epld			
EPLD Device		Version			
MI FPGA		0x7			
IO FPGA		0x17			
MI FPGA2		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
cs2# instal.	l epld bootfla	sh:n9000-epld.9	.3.5.img r	module 1	
Compatibili	ty check:				
		Upgradable	_		
		Yes dis			
Dataina :	7DID	D1			
3		Please wait			
-		ccording to fol	-		
	E ELTD	Running	-version	New-vers	sion Upg-
Required					
1 CIID	MI EDCA	0x07		0x07	No
		0x17		0x19	
	MI FPGA2			0x02	No
	odules require		£ +b		
		led at the end o	or the upg.	rade	
Do you want	to continue (y/n) : [n] y			
Proceeding	to upgrade Mod				
rioceeding	to upgrade mod	uies.			
Starting Mo.	dule 1 EPLD Up	arado			
Starting Mo	aute i Erno op	grade			
Module 1 ·	IO FDCA [Droar	amming] : 100.0	INS 1	61 of	61 sectors)
	LD upgrade is	3 -	000 (04 01	04 Sectors)
module Ty	pe Upgrade-Re	Suit			
1 SU	P Success				
EPLDs upgra	ded.				
Module 1 EP:	LD upgrade is	successful.			

After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

cs2#	show version module 1 epld	
EPLD	Device	Version
MI	FPGA	0x7
	FPGA	0x19
	FPGA2	0x2
GEM	FPGA	0x2

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 9336C-FX2 switch for the first time. You can also use this procedure to upgrade your RCF version.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names arecluster1-01, cluster1-02, cluster1-03, and cluster1-04.
- The cluster LIF names are cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1, and cluster1-04_clus2.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches: network devicediscovery show

		Discovered Device (LLDP: ChassisID)	Interface	Platform
cluster1-0	_			_
C9336C	e0a	cs1	Ethernet1/7	N9K-
C9336C	e0d	0.5.7	Ethernet1/7	NOV-
C9336C	eoa	C32	Ecuerueci//	NJK
cluster1-0	2/cdp			
	_	cs1	Ethernet1/8	N9K-
C9336C				
	e0d	cs2	Ethernet1/8	N9K-
C9336C				
cluster1-0	_			
	e0a	cs1	Ethernet1/1/1	N9K-
C9336C	01	0	D.1 .1/1/1	31077
C9336C	e0b	cs2	Ethernet1/1/1	N9K-
cluster1-0	4/cdn			
01400011 0	_	cs1	Ethernet1/1/2	N9K-
C9336C				
	e0b	cs2	Ethernet1/1/2	N9K-
C9336C				

- 2. Check the administrative and operational status of each cluster port.
 - a. Verify that all the cluster ports are up with a healthy status: network port show -role cluster

Node: clu	ster1-02						
.vode. cra	02						
Ignore							
II a a l ± la						Speed (Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	МТП	Admin/Oper	Status
Status	1156466	Diodadase	Domaii		1110	riamiri, oper	beacub
 e0a	 Cluster	Cluster		un	9000	auto/10000	n
coa healthy f		CIUSCCI		αр	3000	auco, 100000	S
_	Cluster	Cluster		up	9000	auto/100000)
healthy f	alse						
8 entries	were displa	yed.					
Node: clu	ster1-03						
Ignore	<u> </u>						
						Speed(Mbps)	Health
Health							
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
		_				4	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
	Cluster	Cluster		up	9000	auto/10000	healths
false	OT UD CCT	CIGOCCI		αр	3000	4400/10000	iicai cii ₋
Node: clu	ster1-04						
Ignore							
-						Speed(Mbps)	Health
Health	TD	D 1	D .	T ' 1	NATE TO	7.1.1.70	
Port Status	IPspace	Broadcast	Domain	Link	M.T.N	Admin/Oper	Status
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
	Cluster	Cluster		up	9000	auto/10000	health
<pre>false cluster1:</pre>	di S						

b. Verify that all the cluster interfaces (LIFs) are on the home port: network interface show -role

		Logical	Status	Network	Current
Cur	rent Is				
Vse	rver	Interface	Admin/Oper	Address/Mask	Node
	t Hom				
	ster				
CIU	ster	cluster1-01 clus1	un/un	169.254.3.4/23	cluster1-
01	e0a	true	αρ, αρ	103.201.011, 20	01400011
		cluster1-01 clus2	up/up	169.254.3.5/23	cluster1-
01	e0d	true			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-
02	e0a	true			
		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-
02	e0d	true	,	1.60 0.7.1 0.400	
0.2	- 0 -	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-
03	e0a	true cluster1-03 clus2	up/up	169.254.1.1/23	cluster1-
03	e0b	true	up/ up	109.234.1.1/23	Clustell-
0.5	C02	cluster1-04 clus1	up/up	169.254.1.6/23	cluster1-
04	e0a	true			
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-
04	e0b	true			
8 e	ntries w	ere displayed.			

C. Verify that the cluster displays information for both cluster switches: system cluster-switch show -is-monitoring-enabled-operational true

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch
                        Type
                                         Address
                                                        Model
cluster-network 10.233.205.90
cs1
                                                       N9K-
C9336C
    Serial Number: FOCXXXXXXGD
     Is Monitored: true
          Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                 9.3(5)
   Version Source: CDP
cs2
                        cluster-network 10.233.205.91 N9K-
C9336C
    Serial Number: FOCXXXXXXGS
     Is Monitored: true
          Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                 9.3(5)
   Version Source: CDP
cluster1::*>
```

3. Disable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

4. On cluster switch cs2, shut down the ports connected to the cluster ports of the nodes.

```
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
```

5. Verify that the cluster ports have migrated to the ports hosted on cluster switch cs1. This might take a few seconds.network interface show -role cluster

		Logical	Status	Network	Current
Current	_				
Vserver		Interface	Admin/Oper	Address/Mask	Node
Port	_				
Cluster					
0145601		cluster1-01 clus1	up/up	169.254.3.4/23	cluster1-01
e0a	true	 e			
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0a	fals	se			
		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0a	true	е			
		cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0a	fals	se			
		cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0a	true	е			
		cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0a	fals				
		cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0a	true				
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0a		se ere displayed.			

6. Verify that the cluster is healthy: cluster show

Node Health Eligibility Epsil
alvatani 01 tava tava falsa
aluatom1 01 + muo + muo falso
cluster1-01 true true false
cluster1-02 true true false
cluster1-03 true true true
cluster1-04 true true false
4 entries were displayed.
<pre>cluster1::*></pre>

- 7. Clean the configuration on switch cs2 and perform a basic setup.
 - a. Clean the configuration. This step requires a console connection to the switch.

```
cs2# write erase Warning: This command will erase the startup-configuration. Do you wish to proceed anyway? (y/n) [n] y cs2# reload This command will reboot the system. (y/n)? [n] y cs2#
```

- b. Perform a basic setup of the switch.
- 8. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

This example shows TFTP being used to copy an RCF to the bootflash on switch cs2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

9. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

This example shows the RCF file Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt being installed on switch cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config echo-commands
```

10. Examine the banner output from the show banner motd command. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

```
cs2# show banner motd
****************
* NetApp Reference Configuration File (RCF)
* Switch : Nexus N9K-C9336C-FX2
* Filename : Nexus 9336C RCF v1.6-Cluster-HA-Breakout.txt
* Date : 10-23-2020
* Version : v1.6
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int e1/1/1-4,
e1/2/1-4
, e1/3/1-4
* Ports 4-6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int e1/4/1-
4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
* Undo breakout commands and return interfaces to 40/100G configuration
in confi
q mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25q-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
******************
*****
```

11. Verify that the RCF file is the correct newer version: show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

The RCF banner

- The node and port settings
- Customizations
 The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.
- 12. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

13. Reboot switch cs2. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs2# reload This command will reboot the system. (y/n)? [n] y
```

- 14. Verify the health of cluster ports on the cluster.
 - a. Verify that e0d ports are up and healthy across all nodes in the cluster: network port show -role cluster

```
cluster1::*> network port show -role cluster
Node: cluster1-01
Ignore
                                            Speed (Mbps) Health
Health
Port
        IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
_____
e0a
       Cluster
                    Cluster
                                  up
                                        9000 auto/10000 healthy
false
e0b
    Cluster
                    Cluster
                                        9000 auto/10000 healthy
                                   up
false
Node: cluster1-02
Ignore
                                            Speed (Mbps) Health
```

Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a false	 Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
Node: cluster1-03							
Ignore						Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
				up	9000	auto/100000	
healthy feed healthy f	Cluster	Cluster		up	9000	auto/100000	
Node: cluster1-04							
Ignore						Speed(Mbps)	Health
Status	IPspace						Status
healthy f				up	9000	auto/100000	0
e0d Cluster Cluster up 9000 auto/100000 healthy false 8 entries were displayed.							

b. Verify the switch health from the cluster (this might not show switch cs2, since LIFs are not homed on e0d).

cluster1-0	1/cdp				
	e0a	cs1		Ethernet1/7	N9K-
C9336C					
	e0d	cs2		Ethernet1/7	N9K-
C9336C					
cluster01-	2/cdp				
	e0a	cs1		Ethernet1/8	N9K-
C9336C					
	e0d	cs2		Ethernet1/8	N9K-
C9336C					
cluster01-	3/cdp				
	e0a	cs1		Ethernet1/1/1	N9K-
C9336C					
	e0b	cs2		Ethernet1/1/1	N9K-
C9336C					
cluster1-0	4/cdp				
	e0a	cs1		Ethernet1/1/2	N9K-
C9336C					
	e0b	cs2		Ethernet1/1/2	N9K-
cluster1:: -operation		em cluster		-monitoring-enable	d
cluster1:: -operation Switch	al true		-switch show -is Type		
cluster1:: -operation Switch	al true		Type	-monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1	al true		Type	-monitoring-enable	d Mode
cluster1:: -operation Switch cs1 C9336C	al true		Type cluster-network	-monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1 C9336C Seria	al true	r: FOCXXXX	Type cluster-network	-monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1 C9336C Seria	al true	r: FOCXXXX	Type cluster-network	-monitoring-enable Address	d Mode
cluster1:: -operation Switch cs1 C9336C Seria Is M	al true l Number conitorec	f: FOCXXXX d: true n: None	Type cluster-network	-monitoring-enable Address	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M	al true l Number conitorec	f: FOCXXXX d: true n: None	Type cluster-network	-monitoring-enable Address	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M	al true l Number conitorec	f: FOCXXXX d: true n: None	Type cluster-network	-monitoring-enable Address	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version	al true l Number conitorec	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network	-monitoring-enable Address	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version	al true l Number conitored Reasor Versior	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network	-monitoring-enable Address	d Mode NX9-
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio	al true l Number onitored Reasor Versior	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating S	-monitoring-enable Address	d Mode NX9- ware,
cluster1:: -operation Switchcs1 C9336C Seria Is M Software Version Versio	al true l Number onitored Reasor Versior	r: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating S	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria	al true l Number conitored Reasor Versior n Source	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP	Type cluster-network XXXGD Jexus Operating S cluster-network	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft	d Mode NX9- ware,
-operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria	al true l Number onitored Reasor Versior n Source	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP	Type cluster-network XXXGD Jexus Operating S cluster-network	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria	al true l Number conitored Reasor Versior n Source l Number conitored	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP	Type cluster-network XXXGD Jexus Operating S cluster-network	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria Is M Software	al true l Number conitored Reasor Versior n Source l Number conitored Reasor	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP	Type cluster-network XXXGD Jexus Operating S cluster-network	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria Is M Software	al true l Number conitored Reasor Versior n Source l Number conitored Reasor	r: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP r: FOCXXXX d: true n: None n: Cisco N	Type cluster-network XXXGD Jexus Operating S cluster-network	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft 10.233.205.91	d Mode NX9- ware,
cluster1:: -operation Switch cs1 C9336C Seria Is M Software Version Versio cs2 C9336C Seria Is M Software Version	al true l Number conitored Reasor Versior n Source l Number conitored Reasor	f: FOCXXXX d: true n: None n: Cisco N 9.3(5) e: CDP f: FOCXXXX d: true n: None n: Cisco N 9.3(5)	Type cluster-network XXXGD Jexus Operating S cluster-network	-monitoring-enable Address 10.233.205.90 ystem (NX-OS) Soft 10.233.205.91	d Mode NX9- ware,

2 entries were displayed.



You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on VLAN0092. Port consistency restored. 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001. Inconsistent peer vlan. 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

15. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes.

The following example uses the interface example output from step 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

16. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds.

network interface show -role cluster

cluster	1::*> network int	erface show -role	cluster	
	Logical	Status	Network	Current
Current				
	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
	cluster1-01_	clus1 up/up	169.254.3.4/23	cluster1-01
e0d	false			
	cluster1-01_	clus2 up/up	169.254.3.5/23	cluster1-01
e0d	true			
0.1	_	clus1 up/up	169.254.3.8/23	cluster1-02
e0d	false	-12	160 254 2 0/22	ala+a1 00
e0d	cluster1-02_true	ciusz up/up	169.254.3.9/23	cluster1-02
eoa	cluster1-03	clus1 un/un	169.254.1.3/23	cluster1-03
e0b	false	σεασε αργαρ	103,101,10,10	01000011 00
	cluster1-03	clus2 up/up	169.254.1.1/23	cluster1-03
e0b	true			
	cluster1-04_	clus1 up/up	169.254.1.6/23	cluster1-04
e0b	false			
	cluster1-04_	clus2 up/up	169.254.1.7/23	cluster1-04
	true			
	es were displayed	•		
cluster	1::*>			

17. Verify that the cluster is healthy: cluster show

cluster1::*> cluste	r show		
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were disp	layed.		
cluster1::*>			

- 18. Repeat Steps 7 to 14 on switch cs1.
- 19. Enable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

20. Reboot switch cs1. You do this to trigger the cluster LIFs to revert to their home ports. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs1# reload This command will reboot the system. (y/n)? [n] y
```

21. Verify that the switch ports connected to the cluster ports are up.

```
cs1# show interface brief \| grep up
Eth1/1/1
           1
                                                          10G(D)
                  eth access up
                                    none
Eth1/1/2 1 eth access up
                                    none
                                                          10G(D)
Eth1/7
            1
                   eth trunk up
                                                         100G(D)
                                    none
Eth1/8
          1 eth trunk up
                                    none
                                                         100G(D)
--
```

22. Verify that the ISL between cs1 and cs2 is functional: show port-channel summary

23. Verify that the cluster LIFs have reverted to their home port: network interface show -role cluster

Clustel	1.	> network interface Logical	Status		Current
Current	Ts	nogicai	Status	NECMOLY	Cullenc
	_	Interface	Admin/Oper	Address/Mask	Node
Port			110117, 019 01	110.02.000, 110.011	1.0 0.0
Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	true				
		cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true		,	1.60, 054, 0, 0,/00	
0.1		cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	true			160 254 2 0/22	~1~+ ~1 00
e0d	t.rue	_	up/up	169.254.3.9/23	cluster1-02
eva	CIUC	cluster1-03 clus1	11n / 11n	169.254.1.3/23	cluster1-03
e0b	true	_	ир/ ир	107.254.1.5/25	Clustell 05
	CIUC		up/up	169.254.1.1/23	cluster1-03
e0b	true	-	α ρ , α ρ	103,1201,11,1	01000011 00
		cluster1-04 clus1	up/up	169.254.1.6/23	cluster1-04
e0b	true	_			
		cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0b	true	=			
8 entri	es we	ere displayed.			

24. Verify that the cluster is healthy: ${\tt cluster}\ {\tt show}$

cluster1::*> cluster	show		
Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were disp	ayed.		
cluster1::*>			

25. Ping the remote cluster interfaces to verify connectivity: cluster ping-cluster -node local

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03 clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03 clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04 clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04 clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01 clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01 clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02 clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02 clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
. . . . . . . . . . . .
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
   Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Replace a Cisco Nexus 9336C-FX2 cluster switch

Replacing a defective Nexus 9336C-FX2 switch in a cluster network is a nondisruptive procedure (NDU).

Before you begin

The following conditions must exist before performing the switch replacement in the current environment and on the replacement switch.

- Existing cluster and network infrastructure:
 - The existing cluster must be verified as completely functional, with at least one fully connected cluster switch.
 - All cluster ports must be up.
 - All cluster logical interfaces (LIFs) must be up and on their home ports.
 - The ONTAP cluster ping-cluster -node node1 command must indicate that basic connectivity and larger than PMTU communication are successful on all paths.
- Nexus 9336C-FX2 replacement switch:
 - Management network connectivity on the replacement switch must be functional.
 - Console access to the replacement switch must be in place.
 - The node connections are ports 1/1 through 1/34.
 - All Inter-Switch Link (ISL) ports must be disabled on ports 1/35 and 1/36.
 - The desired reference configuration file (RCF) and NX-OS operating system image switch must be loaded onto the switch.
 - Initial customization of the switch must be complete, as detailed in:

Configuring a new Cisco Nexus 9336C-FX2 switch

Any previous site customizations, such as STP, SNMP, and SSH, should be copied to the new switch.

You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.

The examples in this procedure use the following switch and node nomenclature:

- The names of the existing Nexus 9336C-FX2 switches are cs1 and cs2.
- The name of the new Nexus 9336C-FX2 switch is newcs2.
- The node names are node1 and node2.
- The cluster ports on each node are named e0a and e0b.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The prompt for changes to all cluster nodes is cluster1::*>



The following procedure is based on the following cluster network topology:

	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
false							
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: nod	le2						
Ignore							
Health						Speed(Mbps)	Health
	IPspace	Prondenst	Domain	Tink	MITT	Admin/Onor	C+ 2+11C
Status	irspace	BIOAUCASC	DOMATH	ПТПК	MIO	AdiiIII/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
false				-			4
01	01	Cluster		up	9000	auto/10000	healthy
au e	Cluster	CIUDCCI		uρ	2000		
false	cluster were display			αp			4
false 4 entries		yed.					4
false 4 entries	were display	yed. interface sh		erver			
false 4 entries	<pre>were display :*> network :</pre>	yed. interface sh	ow -vse	erver		cer	
false 4 entries cluster1:	were display :*> network in the second seco	yed. interface sh	ow -vse Netwoi	erver rk	Clust	ter Current	
false 4 entries cluster1: Is Vserver	were display :*> network in the second seco	yed. interface sh Status	ow -vse Netwoi	erver rk	Clust	ter Current	Curren
false 4 entries cluster1: Is Vserver Home	were display :*> network in the second seco	yed. interface sh Status	ow -vse Netwoi	erver rk	Clust	ter Current	Curren
false 4 entries cluster1: Is Vserver	:*> network : Logical Interface	yed. interface sh Status Admin/Oper	ow -vse Networ Addres	erver rk ss/Ma:	Clust sk	cer Current Node	Curren Port
false 4 entries cluster1: Is Vserver Home Cluster	:*> network : Logical Interface	yed. interface sh Status	ow -vse Networ Addres	erver rk ss/Ma:	Clust sk	ter Current	Curren
false 4 entries cluster1: Is Vserver Home	:*> network : Logical Interface node1_clus	yed. interface sh Status Admin/Oper	ow -vse Networ Addres	erver rk ss/Ma:	Clust sk 	cer Current Node	Curren Port
false 4 entries cluster1: Is Vserver Home Cluster	:*> network : Logical Interface node1_clus	yed. interface sh Status Admin/Oper	ow -vse Networ Addres	erver rk ss/Ma:	Clust sk 	Current Node	Curren Port e0a
false 4 entries cluster1: Is Vserver Home Cluster	:*> network : Logical Interface nodel_clus	yed. interface sh Status Admin/Oper	ow -vse Networ Addres 169.25	erver rk ss/Ma: 54.20	Clustsk 9.69/1	Current Node 16 node1 16 node1	Curren Port e0a
false 4 entries cluster1: Is Vserver Home Cluster	:*> network : Logical Interface nodel_clus	yed. interface sh Status Admin/Oper s1 up/up	ow -vse Networ Addres 169.25	erver rk ss/Ma: 54.20	Clustsk 9.69/1	Current Node 16 node1 16 node1	Curren Port e0a e0b
false 4 entries cluster1: Is Vserver Home Cluster true	:*> network : Logical Interface node1_clus node2_clus	yed. interface sh Status Admin/Oper s1 up/up	ow -vse Network Addres 169.25 169.25	erver rk ss/Ma: 54.20:	Clustsk 9.69/1	Current Node 16 node1 16 node2	Curren Port e0a e0b
false 4 entries cluster1: Is Vserver Home Cluster true	:*> network : Logical Interface node1_clus node2_clus	yed. interface sh Status Admin/Oper s1 up/up s2 up/up	ow -vse Network Addres 169.25 169.25	erver rk ss/Ma: 54.20:	Clustsk 9.69/1	Current Node 16 node1 16 node2	Current Port e0a e0b e0a
false 4 entries cluster1: Is Vserver Home Cluster true true true	:*> network : Logical Interface node1_clus node2_clus	yed. interface sh Status Admin/Oper s1 up/up s2 up/up s1 up/up	ow -vse Network Addres 169.25 169.25	erver rk ss/Ma: 54.20:	Clustsk 9.69/1	Current Node 16 node1 16 node2	Current Port e0a e0b e0a

e0b cs2 Eth1/2 N9K-C nodel /cdp e0a cs1 Eth1/1 N9K-C e0b cs2 Eth1/1 N9K-C 4 entries were displayed. Cs1# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Br: S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform 1 nodel Eth1/1 144 H FAS2980 6 cs2 Eth1/2 145 H FAS2980 6 cs2 Eth1/35 176 R S I s N9K-C9336C 1 cs2 (FD0220329V5) Eth1/36 176 R S I s N9K-C9336C 1 Total entries displayed: 4 Cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Br: S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform 1 node1 Eth1/1 139 H FAS2980 6 node2 Eth1/2 124 H FAS2980 6		ocal Discovered ort Device (LLDP: Ch	hassisTD) Interfa	ce Platf	orm
e0a cs1 e1h1/2 N9K-0 e0b cs2 Eth1/2 N9K-0 nodel /cdp e0a cs1 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 4 entries were displayed. Ccs1# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Br: S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hidtme Capability Platform incodel Eth1/1 144 H FAS2980 e1 cs2 Eth1/2 145 H FAS2980 e1 cs2(FD0220329V5) Eth1/36 176 R S I s N9K-C9336C incodel Eth1/36 176 R S I s N9K-C9336C incodel entries displayed: 4 Ccs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Br: S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hidtme Capability Platform incodel Eth1/1 139 H FAS2980 e1 nodel Eth1/1 139 H FAS2980 e1					01111
e0a cs1 e1h1/2 N9K-0 e0b cs2 Eth1/2 N9K-0 nodel /cdp e0a cs1 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 4 entries were displayed. Cs1# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Br: S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrice Hidtme Capability Platform indel Eth1/1 144 H FAS2980 e1 node2 Eth1/2 145 H FAS2980 e1 cs2 (FD0220329V5) Eth1/36 176 R S I s N9K-C9336C Indel Eth1/36 Indel Eth1/36 R S I s N9K-C9336C Indel E					
e0b cs2 Eth1/2 N9K-C node1 /cdp e0a cs1 Eth1/1 N9K-C e0b cs2 Eth1/1 N9K-C 4 entries were displayed. Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Br: S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrice Hidtme Capability Platform in the code of t	lp	dp			
nodel /cdp e0a csl Ethl/1 N9K-0 e0b cs2 Ethl/1 N9K-0 dentries were displayed. Csl# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Brise S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrice Hidtme Capability Platform incidel Ethl/1 144 H FAS2980 decended Ethl/2 145 H FAS2980 decended Ethl/35 176 R S I s N9K-C9336C incide Ethl/36 Ethl/36 I I I I I I I I I I I I I I I I I I I	a cs1	0a cs1	Eth1/2	N9K-C	9336C
e0a cs1 Eth1/1 N9K-0 e0b cs2 Eth1/1 N9K-0 4 entries were displayed. Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Briss - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrice Hidtme Capability Platform in the code of the code	b cs2	0b cs2	Eth1/2	N9K-C	9336C
e0b cs2 Eth1/1 N9K-0 4 entries were displayed. Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Briss S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hidtme Capability Platform Incide1 Eth1/1 144 H FAS2980 6	lp	dp			
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Briss S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Indel Eth1/1 144 H FAS2980 6 Esc2 Eth1/2 145 H FAS2980 6 Esc2 Eth1/35 176 R S I s N9K-C9336C Indel Eth1/36 Indel Eth1/4 Indel Eth1/1 Indel Eth1/Indel Eth1/1 Indel Eth1/Indel Indel Indel Indel Indel Indel Indel Indel Inde	a cs1	0a cs1	Eth1/1	N9K-C	9336C
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Source-Route-Bridge, B - Source-Route-Bridge, B - Source-Route-Bridge, B - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID	b cs2	0b cs2	Eth1/1	N9K-C	9336C
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Supports-STP-Dispute Device-ID	display	e displayed.			
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Supports-STP-Dispute Device-ID					
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Supports-STP-Dispute Device-ID					
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Bridge Eth1/1 144 H FAS2980 Groupe Eth1/2 145 H FAS2980 Groupe Eth1/35 176 R S I s N9K-C9336C Frotal entries displayed: 4 Device-ID Router, T - Trans-Bridge, B - Source-Route-Bridge S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Indicated Eth1/1 139 H FAS2980 Groupe Eth1/2 124					
S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform nodel Eth1/1 144 H FAS2980 e cs2 Eth1/2 145 H FAS2980 f cs2 Eth1/35 176 R S I s N9K-C9336C H cs2(FD0220329V5) Eth1/36 176 R S I s N9K-C9336C H Cs2(FD0220329V5) Eth1/36 176 R S I s N9K-C9336C H Cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform nodel Eth1/1 139 H FAS2980 e code2 Eth1/2 124 H FAS2980 e	neighbor	neighbors			
S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform December 1	l B	d D D T	B	Q	-1
V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Incodel Eth1/1 144 H FAS2980 6 Decode Eth1/2 145 H FAS2980 7 Decode Eth1/35 176 R S I S N9K-C9336C FACE ETH1/36 PROBLEM ETH1/3 PROBLEM ETH1/39 PROBLEM			_		age
s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Incode1 Eth1/1 144 H FAS2980 6 Decode2 Eth1/2 145 H FAS2980 6 Desc2 Eth1/35 176 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB SEC (FD0220329V5) Eth1/36 R S I S N9K-C9336C FEB				_	
Device-ID Local Intrfce Hldtme Capability Platform Incodel Eth1/1 144 H FAS2980 6 mode2 Eth1/2 145 H FAS2980 6 mode2 Eth1/35 176 R S I S N9K-C9336C Incode Intrfce Hldtme Capability Platform Incode Incode Intrfce Hldtme Capability Platform Incode				ged-Device,	
node1 Eth1/1 144 H FAS2980 6 node2 Eth1/2 145 H FAS2980 6 cs2 Eth1/35 176 R S I s N9K-C9336C F cs2(FD0220329V5) Eth1/36 176 R S I s N9K-C9336C F Cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Brise S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Indel Eth1/1 139 H FAS2980 6 node2 Eth1/2 124 H FAS2980 6	s -	s - Supports-STP-	-Dispute		
mode2 Eth1/2 145 H FAS2980 6 cs2 Eth1/35 176 R S I s N9K-C9336C F cs2(FD0220329V5) Eth1/36 176 R S I s N9K-C9336C F Total entries displayed: 4 cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Brist S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Indel Eth1/1 139 H FAS2980 6 mode2 Eth1/2 124 H FAS2980 6	Loc	Local Intrfce F	Hldtme Capability	Platform P	ort II
Es2 Eth1/35 176 R S I S N9K-C9336C Es2(FD0220329V5) Eth1/36 176 R S I S N9K-C9336C Es2(FD0220329V5) Eth1/36 176 R S I S N9K-C9336C Es2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Brise S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Incode1 Eth1/1 139 H FAS2980 60 100 100 100 100 100 100 100 100 100	Eth	Eth1/1 1	144 н	FAS2980 e	0a
Cs2(FDO220329V5) Eth1/36 176 R S I s N9K-C9336C F Total entries displayed: 4 Cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Brise S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Incode1 Eth1/1 139 H FAS2980 6 node2 Eth1/2 124 H FAS2980 6	Eth	Eth1/2	145 Н	FAS2980 e	0a
Total entries displayed: 4 cs2# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Brise S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform node1 Eth1/1 139 H FAS2980 6 node2 Eth1/2 124 H FAS2980	Eth	Eth1/35	176 RSIs	N9K-C9336C E	th1/35
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Source-Route-Bridge	75) Eth				th1/3
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge, B - Source-Route-Bridge					
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Briss S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Hodel Eth1/1 139 H FAS2980 Eth1/2 124 H FAS2980	displaye	displayed: 4			
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Briss S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform node1 Eth1/1 139 FAS2980 Eth1/2 124 H FAS2980					
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Briss S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform node1 Eth1/1 139 FAS2980 Eth1/2 124 H FAS2980					
S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Indel Eth1/1 139 H FAS2980 Facebook FAS2980 Facebook FAS2980 F	neighbor	neighbors			
S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Indel Eth1/1 139 H FAS2980 Facebook FAS2980 Facebook FAS2980 F	les· R -	des: R - Router. T - 5	Trans-Bridge B -	Source-Route-Bri	dae
V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Incodel Eth1/1 139 H FAS2980 Facebook FAS2980 FAS298			- ·		age
s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform I node1 Eth1/1 139 H FAS2980 ende2 Eth1/2 124 H FAS2980 ende2		•		<u>-</u>	
Device-ID Local Intrfce Hldtme Capability Platform Incodel Eth1/1 139 H FAS2980 encode2 Eth1/2 124 H FAS2980				jed-Device,	
node1 Eth1/1 139 H FAS2980 e node2 Eth1/2 124 H FAS2980 e	S -	s - supports-STP-	-птэћисе		
nodel Eth1/1 139 H FAS2980 e node2 Eth1/2 124 H FAS2980 e	Loc	Local Intrice	Hldtme Capability	Platform P	ort II
node2 Eth1/2 124 H FAS2980					010 11 0b
	_	·			0b
COT TIGHT OF TABLE TO THE DESCRIPTION TO THE DESCRI					ob th1/3:
					th1/3

Total entries displayed: 4

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Install the appropriate RCF and image on the switch, newcs2, and make any necessary site preparations.

If necessary, verify, download, and install the appropriate versions of the RCF and NX-OS software for the new switch. If you have verified that the new switch is correctly set up and does not need updates to the RCF and NX-OS software, continue to step 2.

- a. Go to the NetApp Cluster and Management Network Switches Reference Configuration File Description Page on the NetApp Support Site.
- b. Click the link for the *Cluster Network and Management Network Compatibility Matrix*, and then note the required switch software version.
- c. Click your browser's back arrow to return to the Description page, click **CONTINUE**, accept the license agreement, and then go to the Download page.
- d. Follow the steps on the Download page to download the correct RCF and NX-OS files for the version of ONTAP software you are installing.
- 3. On the new switch, log in as admin and shut down all of the ports that will be connected to the node cluster interfaces (ports 1/1 to 1/34).

If the switch that you are replacing is not functional and is powered down, go to Step 4. The LIFs on the cluster nodes should have already failed over to the other cluster port for each node.

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-34
newcs2(config-if-range)# shutdown
```

4. Verify that all cluster LIFs have auto-revert enabled: network interface show -vserver Cluster -fields auto-revert

5. Verify that all the cluster LIFs can communicate: cluster ping-cluster

```
cluster1::*> cluster ping-cluster node1
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e0a
Cluster node1 clus2 169.254.49.125 node1 e0b
Cluster node2 clus1 169.254.47.194 node2 e0a
Cluster node2 clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Shut down the ISL ports 1/35 and 1/36 on the Nexus 9336C-FX2 switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/35-36
cs1(config-if-range)# shutdown
cs1(config-if-range)#
```

- 7. Remove all of the cables from the Nexus 9336C-FX2 cs2 switch, and then connect them to the same ports on the Nexus C9336C-FX2 newcs2 switch.
- 8. Bring up the ISLs ports 1/35 and 1/36 between the cs1 and newcs2 switches, and then verify the port channel operation status.

Port-Channel should indicate Po1(SU) and Member Ports should indicate Eth1/35(P) and Eth1/36(P).

This example enables ISL ports 1/35 and 1/36 and displays the port channel summary on switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config) \# int e1/35-36
cs1(config-if-range) # no shutdown
csl(config-if-range)# show port-channel summary
Flags: D - Down
                  P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
               Type Protocol Member Ports
Group Port-
     Channel
_____
1 Po1(SU) Eth LACP Eth1/35(P) Eth1/36(P)
cs1(config-if-range)#
```

9. Verify that port e0b is up on all nodes: network port show ipspace Cluster

The output should be similar to the following:

<pre>cluster1::*> network port show -ipspace Cluster</pre>										
Node: node1										
Ignore						G 1/26				
Health						Speed (Mbps)	Health			
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status			
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy			
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy			
Taise										
Node: nod	e2									
Ignore										
						Speed (Mbps)	Health			
Health	IPspace	Prondenst	Domain	Tiple	Mmti	Admin/Onon	2+2+110			
Status	irspace	Bloadcast	DOMATH	ТПК	MIO	Admin/Oper	Status			
	Cluster	Cluster		up	9000	auto/10000	healthy			
	Cluster	Cluster		up	9000	auto/auto	-			
false										
4 entries	were display	ed.								

10. On the same node you used in the previous step, revert the cluster LIF associated with the port in the previous step by using the network interface revert command.

In this example, LIF node1_clus2 on node1 is successfully reverted if the Home value is true and the port is e0b.

The following commands return LIF node1_clus2 on node1 to home port e0a and displays information about the LIFs on both nodes. Bringing up the first node is successful if the Is Home column is true for both cluster interfaces and they show the correct port assignments, in this example e0a and e0b on node1.

cluster1::*	> network int	erface show	-vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	nodel_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0a
false					
1 ontrios w	oro displayed				
4 encires we	ere displayed	•			

11. Display information about the nodes in a cluster: cluster show

This example shows that the node health for node1 and node2 in this cluster is true:

```
Cluster1::*> cluster show

Node Health Eligibility
-----
node1 false true
node2 true true
```

12. Verify that all physical cluster ports are up: network port show ipspace Cluster

<pre>cluster1::*> network port show -ipspace Cluster</pre>								
Node node Ignore	1							
-					Speed(Mbps)	Health		
Health					- 1 - 1 - 10			
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status		
Status								
e0a	Cluster	Cluster	up	9000	auto/10000	healthy		
false			_			_		
e0b	Cluster	Cluster	up	9000	auto/10000	healthy		
false								
Node: nod Ignore	e2							
3					Speed (Mbps)	Health		
Health								
Port	IPspace	Broadcast Domair	Link	MTU	Admin/Oper	Status		
Status								
e0a	Cluster	Cluster	up	9000	auto/10000	healthy		
false								
e0b false	Cluster	Cluster	up	9000	auto/10000	healthy		
4 entries	were displa	yed.						

^{13.} Verify that all the cluster LIFs can communicate: ${\tt cluster}\ {\tt ping-cluster}$

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e0a
Cluster node1 clus2 169.254.49.125 node1 e0b
Cluster node2 clus1 169.254.47.194 node2 e0a
Cluster node2 clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

14. Confirm the following cluster network configuration: network port show

Ignore								
_ 5					Speed	d (Mbp	5)	Health
Health								
Port	IPspace		Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status								
e0a	Cluster		Cluster		up	9000	auto/10000	healthy
false								
e0b	Cluster		Cluster		up	9000	auto/10000	healthy
false								
4 entries	were dis	nlave	d					
1 01101105	were arb	ртаус	u •					
cluster1:	:*> netwo	rk in	terface sl	now -vs	erver	Clust	ter	
	Taniaa	7	C+ - + · · ·	Notre]_		C	
Current Is	-	1	Status	Netwo:	rĸ		Current	
Vserver		ace	Admin/Ope:	r Addre	ss/Mas	sk	Node	Port
Home					·			
Cluster	nodo1	alua1	11n /11n	160 2	54 200	0 60/	16 nodel	e0a
true	node1_	CIUSI	up/ up	109.2	J4 • Z U .	9.09/.	ro noder	eua
0200	node1	clus2	up/up	169.2	54.49	.125/	16 node1	e0b
true								
	node2_	clus1	up/up	169.2	54.47	.194/	16 node2	e0a
true	1 0		,	1.60.0	F 4 1 0	100/	1.6	0.1
true	node2_	Clusz	up/up	169.2	54.19	.183/.	16 node2	e0b
crue								
4 entries	were dis	playe	d.					
cluster1:	:> networ	k dev	ice-disco	very sh	gd- wc	rotoc	ol cdp	
Nodo /	T c c c l	D:	orro no si					
Node/ Protocol				Chassi	sID)	Inte	rface	Platform
								LIGOTOTIII
node2	/cdp							
	e0a	cs1				0/2		N9K-
C9336C	- 01		- 0			0.70		NI OIZ
C9336C	e0b	newc	SZ			0/2		N9K-
093300								

node1	/cdp			0./1		
202262	e0a	cs1		0/1	N9	K-
C9336C	- 01-			0 /1	210	T.7
C9336C	aue	newcs2		0/1	N9	K-
C9336C						
4 entries	were di	splayed.				
cs1# show	cdp nei	ghbors				
Canability	Codos	R - Router, T -	Trans-	Pridao P -	Courgo-Pouto-	Pridao
Capability	codes:	S - Switch, H -		_		bilage
		V - VoIP-Phone,			-	
		s - Supports-ST			ca 201100 ,	
			-1			
Device-ID Port ID		Local Intrfc	e Hldt	me Capabilit	y Platform	
node1		Eth1/1	144	Н	FAS2980	e0a
node2		Eth1/2	145	Н	FAS2980	e0a
newcs2		Eth1/35	176	RSIs	N9K-C9336C	
Eth1/35						
newcs2		Eth1/36	176	RSIs	N9K-C9336C	
Eth1/36						
Total entr	ias dis	nlaved: A				
iotai enti	ies dis	prayed. 4				
cs2# show	cdp nei	ghbors				
Capability	Codes:	R - Router, T -		J .		Bridge
		S - Switch, H -	•	·	-	
		V - VoIP-Phone,			ed-Device,	
		s - Supports-ST	P-Dispu	te		
Device-ID		Local Intrfce	Hldtme	Capability	Platform	Port
ID		Local Inclice	III a cinc	σαραστίτος	1140101111	1010
node1		Eth1/1	139	Н	FAS2980	e0b
node2		Eth1/2	124	Н	FAS2980	e0b
cs1		Eth1/35	178	RSIs	N9K-C9336C	
Eth1/35						
cs1		Eth1/36	178	R S I s	N9K-C9336C	
Eth1/36						

Total entries displayed: 4

15. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system switch ethernet log setup-password and system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

16. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: csl
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

17. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Replace a Cisco Nexus 9336C-FX2 storage switch

You must be aware of certain configuration information, port connections and cabling requirements when you replace Cisco Nexus 9336C-FX2 storage switches.

Before you begin

You must verify that the following conditions exist before installing the NX-OS software and RCFs on a Cisco Nexus 9336C-FX2 storage switch:

- Your system can support Cisco Nexus 9336C-FX2 storage switches.
- You must have consulted the switch compatibility table on the Cisco Ethernet Switch page for the supported ONTAP, NX-OS, and RCF versions.



You should be aware that there can be dependencies between command syntax in the RCF and NX-OS versions.

- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures.
 Cisco Nexus 3000 Series Switches
- You must have downloaded the applicable RCFs.

About this task

The existing network configuration must have the following characteristics:

- The Cisco Ethernet Switches page has the latest RCF and NX-OS versions on your switches.
- · Management connectivity must exist on both switches.



Make sure that all troubleshooting steps have been completed to confirm that your switch needs replacing.

The replacement Cisco Nexus 9336C-FX2 switch must have the following characteristics:

- · Management network connectivity must be functional.
- Console access to the replacement switch must be in place.
- The appropriate RCF and NX-OS operating system image must be loaded onto the switch.
- Initial customization of the switch must be complete.

Procedure summary

This procedure replaces the second Nexus 9336C-FX2 storage switch S2 with the new 9336C-FX2 switch NS2. The two nodes are node1 and node2.

Steps to complete:

- · Confirm the switch to be replaced is S2.
- · Disconnect the cables from switch S2.
- · Reconnect the cables to switch NS2.
- · Verify all device configurations on switch NS2.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

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

x is the duration of the maintenance window in hours.

2. Check on the health status of the storage node ports to make sure that there is connection to storage switch S1:

storage port show -port-type ENET

storage::*>	storage	port	show -poi	rt-type	ENET		
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
storage::*>							

3. Verify that storage switch S1 is available:

network device-discovery show

```
storage::*> network device-discovery show
Node/
        Local Discovered
Protocol Port Device (LLDP: ChassisID) Interface Platform
-----
         ____
                                    _____
node1/cdp
         e3a S1
                                    Ethernet1/1 NX9336C
         e4a node2
                                    e4a
                                             AFF-A700
         e4e node2
                                            AFF-A700
                                    e4e
node1/11dp
         e3a S1
                                    Ethernet1/1 -
         e4a node2
                                    e4a
             node2
         e4e
                                    e4e
node2/cdp
         e3a S1
                                    Ethernet1/2 NX9336C
         e4a node1
                                    e4a
                                             AFF-A700
         e4e node1
                                             AFF-A700
                                    e4e
node2/11dp
                                    Ethernet1/2 -
         e3a S1
         e4a node1
                                    e4a
         e4e node1
                                    e4e
storage::*>
```

4. Run the show lldp neighbors command on the working switch to confirm that you can see both nodes and all shelves:

show lldp neighbors

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time
                                      Capability
                                                   Port ID
node1
              Eth1/1
                          121
                                      S
                                                   e3a
node2
              Eth1/2
                          121
                                      S
                                                   еЗа
SHFGD2008000011 Eth1/5
                          121
                                      S
                                                   e0a
SHFGD2008000011 Eth1/6
                          120
                                      S
                                                   e0a
SHFGD2008000022 Eth1/7
                          120
                                      S
                                                   e0a
SHFGD2008000022 Eth1/8
                          120
                                                   e0a
                                       S
```

5. Verify the shelf ports in the storage system:

storage shelf port show -fields remote-device, $\operatorname{remote-port}$

- 6. Remove all cables attached to storage switch S2.
- 7. Reconnect all cables to the replacement switch NS2.
- 8. Recheck the health status of the storage node ports: storage port show -port-type ENET

storage::*> sto	5 - 1		1	Speed			VLAN
Node	Port	Type	Mode	-	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
storage::*>							

Verify that both switches are available: network device-discovery show

```
storage::*> network device-discovery show
Node/ Local Discovered
Protocol Port Device (LLDP: ChassisID) Interface Platform
_____
                                    _____
node1/cdp
                                    Ethernet1/1 NX9336C
        e3a S1
        e4a node2
                                    e4a
                                             AFF-A700
        e4e node2
                                    e4e
                                             AFF-A700
        e7b NS2
                                    Ethernet1/1 NX9336C
node1/11dp
        e3a S1
                                    Ethernet1/1 -
                                    e4a
        e4a node2
        e4e node2
                                    e4e
        e7b NS2
                                    Ethernet1/1 -
node2/cdp
                                    Ethernet1/2 NX9336C
        e3a S1
        e4a node1
                                    e4a
                                             AFF-A700
        e4e node1
                                    e4e
                                             AFF-A700
        e7b NS2
                                    Ethernet1/2 NX9336C
node2/11dp
        e3a S1
                                    Ethernet1/2 -
        e4a node1
                                    e4a
        e4e node1
                                    e4e
        e7b NS2
                                    Ethernet1/2 -
storage::*>
```

10. Verify the shelf ports in the storage system:

storage shelf port show -fields remote-device, remote-port

```
storage::*> storage shelf port show -fields remote-device, remote-port
shelf id remote-port remote-device
      __
            -----
3.20
      0 Ethernet1/5
                          S1
3.20
          Ethernet1/5
      1
                          NS2
3.20
     2 Ethernet1/6
                         S1
3.20
     3
          Ethernet1/6
                         NS2
3.30
     0 Ethernet1/7
1 Ethernet1/7
                          S1
3.20
                          NS2
3.30
     2
          Ethernet1/8
                          S1
         Ethernet1/8
3.20 3
                          NS2
storage::*>
```

11. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Cisco 9336C-FX2 shared switch overview

From ONTAP 9.9.1, you can use Cisco Nexus 9336C-FX2 switches to combine storage and cluster functionality into a shared switch scenario.

Setup and configuration guide for Cisco shared switches

Switches supported by ONTAP

From ONTAP 9.9.1, you can use Cisco Nexus 9336C-FX2 switches to combine storage and cluster functionality into a shared switch scenario. If you want to build ONTAP networks with more than two nodes, you need two supported network switches.

The following Cisco shared network switches are supported.

Nexus 9336C-FX2

You can install the Cisco Nexus 9336C-FX2 switch (X190200/X190210) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following table lists the part number and description for the 9336C-FX2 switch, fans, and power supplies:

Part number	Description
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Accessory Kit X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100W PSU - Port side exhaust airflow
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100W PSU - Port side Intake airflow
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, Port side exhaust airflow
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, Port side intake airflow

Setup the switches

If you do not already have the required configuration information and documentation, you need to gather that information before setting up your shared switches.

Before you begin

• You must have access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.

You must have the required shared switch documentation.

See Required documentation for shared switches for more information.

• You must have the required controller documentation and ONTAP documentation.

See NetApp ONTAP documentation.

- You must have the applicable licenses, network and configuration information, and cables.
- You must have the completed cabling worksheets.



In addition to cabling graphics, this guide does provide sample worksheets with recommended port assignments and blank worksheets that you can use to set up your network. For more information, refer to the Hardware Universe.

About this task

All Cisco shared switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software but do not have the RCFs loaded.



You must download the applicable NetApp RCFs from the NetApp Support Site for the switches that you receive.

Procedure

- Rack the switches and controllers. See the Installing a Cisco Nexus 9336C-FX2 cluster switch and pass-through panel in a NetApp cabinet guide for instructions to install the switch in a NetApp cabinet.
- 2. Power on the switches and controllers.
- 3. Perform an initial configuration of the switches based on information provided in Required configuration information.
- 4. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
- 5. Check the software version on the switches, and if necessary, download the NetApp-supported version of the software to the switches.

If you download the NetApp-supported version of the software, then you must also download the NetApp Network Switch Reference Configuration File and merge it with the configuration you saved in Step 3. You can download the file and the instructions from the Cisco Ethernet Switches page.

If you have your own switches, refer to the Cisco site.

Required configuration information

For configuration, you need the appropriate number and type of cables and cable connectors for your switches. Depending on the type of switch you are initially configuring, you need to connect to the switch console port with the included console cable; you also need to provide specific network information.

Required network information for all switches

- You need the following network information for all switch configurations:
 - IP subnet for management network traffic

- Host names and IP addresses for each of the storage system controllers and all applicable switches
- Most storage system controllers are managed through the e0M interface by connecting to the Ethernet service port (wrench icon). On AFF A800 and AFF A700 systems, the e0M interface uses a dedicated Ethernet port.
- Refer to the Hardware Universe for the latest information.

Required network information for Cisco Nexus 9336C-FX2 switches

For the Cisco Nexus 9336C-FX2 switch, you need to provide applicable responses to the following initial setup questions when you first boot the switch. Your site's security policy defines the responses and services to enable:

1. Abort Auto Provisioning and continue with normal setup? (yes/no)

Respond with yes. The default is no.

2. Do you want to enforce secure password standard? (yes/no)

Respond with yes. The default is yes.

3. Enter the password for admin.

The default password is admin; you must create a new, strong password.

A weak password can be rejected.

4. Would you like to enter the basic configuration dialog? (yes/no)

Respond with **yes** at the initial configuration of the switch.

5. Create another login account? (yes/no)

Your answer depends on your site's policies on alternate administrators. The default is no.

6. Configure read-only SNMP community string? (yes/no)

Respond with no. The default is no.

7. Configure read-write SNMP community string? (yes/no)

Respond with **no**. The default is no.

8. Enter the switch name.

The switch name is limited to 63 alphanumeric characters.

9. Continue with out-of-band (mgmt0) management configuration? (yes/no)

Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip address

10. Configure the default-gateway? (yes/no)

Respond with yes. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.

11. Configure advanced IP options? (yes/no)

Respond with no. The default is no.

12. Enable the telnet service? (yes/no)

Respond with no. The default is no.

13. Enable SSH service? (yes/no)

Respond with yes. The default is yes.



SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.

- 14. Enter the type of SSH key you want to generate (dsa/rsa/rsa1). The default is rsa.
- 15. Enter the number of key bits (1024- 2048).
- 16. Configure the NTP server? (yes/no)

Respond with no. The default is no.

17. Configure default interface layer (L3/L2):

Respond with L2. The default is L2.

18. Configure default switch port interface state (shut/noshut):

Respond with **noshut**. The default is noshut.

19. Configure CoPP system profile (strict/moderate/lenient/dense):

Respond with **strict**. The default is strict.

20. Would you like to edit the configuration? (yes/no)

You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered. Respond with no at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.

21. Use this configuration and save it? (yes/no)

Respond with **yes** to save the configuration. This automatically updates the kickstart and system images.



If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

For more information about the initial configuration of your switch, see the following guide: Cisco Nexus 9336C-FX2 Installation and Upgrade Guide.

Required documentation for shared switches

You need specific switch and controller documentation to set up your ONTAP network.

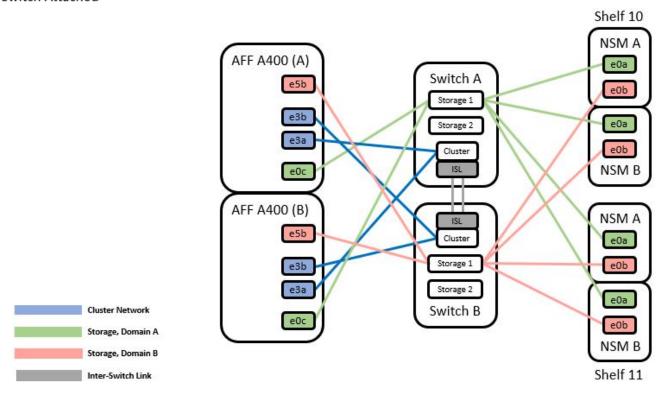
To set up the Cisco Nexus 9336C-FX2 shared switches, see the Cisco Nexus 9000 Series Switches Support page.

Document title	Description
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX- OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

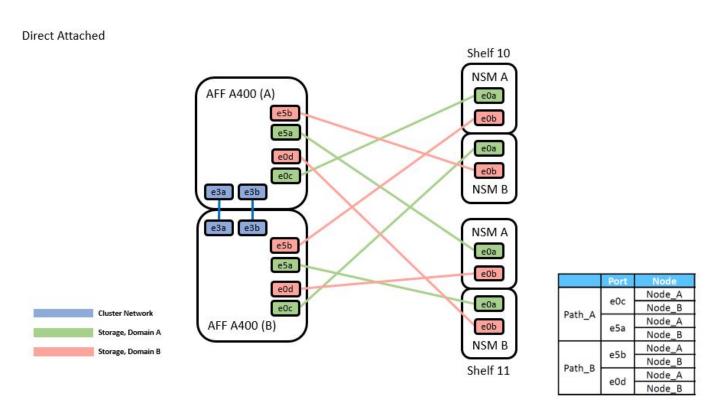
Cisco Nexus 9336C-FX2 cabling details

You can use the following cabling images to complete the cabling between the controllers and the switches.

Switch Attached



If you want to cable storage as direct-attached instead of using the shared switch storage ports, follow the direct-attached diagram:



Cisco Nexus 9336C-FX2 cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using completed sample cabling worksheet as a guide.

The sample port definition on each pair of switches is as follows:

	Switch A			Switch B	
Switch Port	Port Role	Port Usage	Switch Port	Port Role	Port Usage
1	Cluster	40/100GbE	1	Cluster	40/100GbE
2	Cluster	40/100GbE	2	Cluster	40/100GbE
3	Cluster	40/100GbE	3	Cluster	40/100GbE
4	Cluster	40/100GbE	4	Cluster	40/100GbE
5	Cluster	40/100GbE	5	Cluster	40/100GbE
6	Cluster	40/100GbE	6	Cluster	40/100GbE
7	Cluster	40/100GbE	7	Cluster	40/100GbE
8	Cluster	40/100GbE	8	Cluster	40/100GbE
9	Cluster	40GbE w/4x10GbE b/o	9	Cluster	40GbE w/4x10GbE b/o
10	Cluster	100GbE w/4x25GbE b/o	10	Cluster	100GbE w/4x25GbE b/o
11	Storage	100GbE	11	Storage	100GbE
12	Storage	100GbE	12	Storage	100GbE
13	Storage	100GbE	13	Storage	100GbE
14	Storage	100GbE	14	Storage	100GbE
15	Storage	100GbE	15	Storage	100GbE
16	Storage	100GbE	16	Storage	100GbE
17	Storage	100GbE	17	Storage	100GbE
18	Storage	100GbE	18	Storage	100GbE
19	Storage	100GbE	19	Storage	100GbE
20	Storage	100GbE	20	Storage	100GbE
21	Storage	100GbE	21	Storage	100GbE
22	Storage	100GbE	22	Storage	100GbE
23	Storage	100GbE	23	Storage	100GbE
24	Storage	100GbE	24	Storage	100GbE
25	Storage	100GbE	25	Storage	100GbE
26	Storage	100GbE	26	Storage	100GbE
27	Storage	100GbE	27	Storage	100GbE
28	Storage	100GbE	28	Storage	100GbE
29	Storage	100GbE	29	Storage	100GbE
30	Storage	100GbE	30	Storage	100GbE
31	Storage	100GbE	31	Storage	100GbE
32	Storage	100GbE	32	Storage	100GbE
33	Storage	100GbE	33	Storage	100GbE
34	Storage	100GbE	34	Storage	100GbE
35	ISL	100GbE	35	ISL	100GbE
36	ISL	100GbE	36	ISL	100GbE

Where:

- 100G ISL to switch A port 35
- 100G ISL to switch A port 36
- 100G ISL to switch B port 35
- 100G ISL to switch B port 36

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The Supported Cluster Connections table of the Hardware Universe defines the cluster ports used by the platform.

	Switch A			Switch B	
Switch Port	Port Role	Port Usage	Switch Port	Port Role	Port Usage
1			1		
2			2		
3			3		
4			4		
5			5		
6			6		
7			7		
8			8		
9			9		
10			10		
11			11		
12			12		
13			13		
14			14		
15			15		
16			16		
17			17		
18			18		
19			19		
20			20		
21			21		
22			22		
23			23		
24			24		
25			25		
26			26		
27			27		
28			28		
29			29		
30			30		
31			31		
32			32		
33			33		
34			34		
35			35		
36			36		

Where:

- 100G ISL to switch A port 35
- 100G ISL to switch A port 36
- 100G ISL to switch B port 35
- 100G ISL to switch B port 36

Install NX-OS software and RCFs

Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 switches

The Cisco NX-OS software and reference configuration file (RCF) must be installed on Cisco Nexus 9336C-FX2 cluster switches.

Before you begin

The following conditions must exist before you install the NX-OS software and RCF on the cluster switch:

- The cluster must be fully functioning (there should be no errors in the logs or similar issues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have a console connection to the switch, required when installing the RCF.
- You must have consulted the switch compatibility table on the Cisco Ethernet switch page for the supported ONTAP, NX-OS, and RCF versions.
 - See Cisco Ethernet Switches for more information.
- There can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on Cisco Nexus 9000 Series Switches.
 - See Cisco Nexus 9000 Series Switches for more information.
- · You must have the current RCF.

Initial setup

The examples in this procedure use two nodes. These nodes use two 100GbE cluster interconnect ports e3a and e3b, as per the A400 controller.

See the Hardware Universe to verify the correct cluster ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are *cluster1-01* and *cluster1-02*.
- The cluster LIF names are *cluster1-01_clus1* and *cluster1-01_clus2* for cluster1-01 and *cluster1-02_clus1* and *cluster1-02_clus2* for cluster1-02.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport

 $\pmb{\text{message:}} \text{ system node autosupport invoke -node *-type all -message MAINT=x h}$

Where x is the duration of the maintenance window in hours.

2. Change the privilege level to advanced, entering y when prompted to continue:

set -privilege advanced

The advanced prompt (*>) appears.

3. Display how many cluster interconnect interfaces are configured in each node for each cluster interconnect switch:

network device-discovery show -protocol cdp

Clusterl:: Node/		Discove		ery show -pr	otocol cap	
Protocol	Port	Device	(LLDP:	ChassisID)	Interface	Platform
cluster1-0	2/cdp					
	e3a	cs1			Eth1/2	N9K-C9336C
	e3b	cs2			Eth1/2	N9K-C9336C
cluster1-0	1/cdp					
	e3a	cs1			Eth1/1	N9K-C9336C
	e3b	cs2			Eth1/1	N9K-C9336C
4 entries	were dis	plaved.				

- 4. Check the administrative or operational status of each cluster interface:
 - a. Display the network port attributes:

network port show -ipspace Cluster

	luster1-02	port show -	грарасс	CIUS	CCI		
						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e3a	Cluster	Cluster		up	9000	auto/100000	healthy
e3b	Cluster	Cluster		up	9000	auto/100000	healthy
Node: c	luster1-01						
						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e3a	Cluster	Cluster		up	9000	auto/100000	healthy
e3b	Cluster	Cluster		up	9000	auto/100000	healthy
4 entrie	es were displa	ayed.					

b. Display information about the LIFs:

network interface show - vserver Cluster

	Logical	Status	Network	Current	
Current	Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	cluster1-01_clus1	up/up	169.254.209.69/16	cluster1-01	e3a
true					
	cluster1-01_clus2	up/up	169.254.49.125/16	cluster1-01	e3b
true					
	cluster1-02_clus1	up/up	169.254.47.194/16	cluster1-02	e3a
true					
	cluster1-02_clus2	up/up	169.254.19.183/16	cluster1-02	e3b
true					

5. Ping the remote cluster LIFs:

cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node cluster1-02
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01 clus1 169.254.209.69 cluster1-01
                                                           еЗа
Cluster cluster1-01 clus2 169.254.49.125 cluster1-01
                                                           e3b
Cluster cluster1-02 clus1 169.254.47.194 cluster1-02
                                                           e3a
Cluster cluster1-02 clus2 169.254.19.183 cluster1-02
                                                           e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Verify that the auto-revert command is enabled on all cluster LIFs: network interface show - vserver Cluster -fields auto-revert

- 7. Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the following commands:
 - ° system switch ethernet log setup-password
 - ° system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the cluster?
\{y \mid n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the NX-OS software on a Cisco Nexus 9336C- FX2 cluster switch

You can use this procedure to install the NX-OS software on the Cisco Nexus 9336C-FX2 cluster switch.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

Copy the NX-OS software and EPLD images to the Nexus 9336C-FX2 switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
```

4. Verify the running version of the NX-OS software:

show version

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including but
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
  BIOS compile time: 05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]
Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FOC20291J6K
  Device name: cs2
               53298520 kB
  bootflash:
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

- 5. Install the NX-OS image.
- (i)

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[############### 100% -- SUCCESS
Verifying image type.
[################ 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[############### 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[############### 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
_____
               disruptive
         yes
                                   reset
                                            default upgrade is not
hitless
Images will be upgraded according to following table:
        Image Running-Version(pri:alt
                                                    New-Version
Module
Upg-
Required
 1
       nxos 9.3(4)
                                                     9.3(5)
ves
       bios v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020) yes
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.
```

show version	sion of NX-OS soπware aπe	Title switch has repooled.	

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including but
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 05.33
  NXOS: version 9.3(5)
  BIOS compile time: 09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FOC20291J6K
  Device name: cs2
               53298520 kB
  bootflash:
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 277524 usecs after Mon Nov 2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

```
cs2# show version module 1 epld
EPLD Device
                        Version
____ ______
MI FPGA
IO FPGA
                          0x17
MI FPGA2
                          0x2
GEM FPGA
                          0x2
GEM FPGA
                          0x2
GEM FPGA
                          0x2
GEM FPGA
                          0x2
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module Type Upgradable Impact Reason
_____
       SUP Yes disruptive Module Upgradable
Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module Type EPLD
                          Running-Version New-Version Upg-
Required
_____ ______
   1 SUP MI FPGA 0x07
1 SUP IO FPGA 0x17
                                        0x07
                                                  No
                                        0x19
                                                  Yes
   1 SUP MI FPGA2
                         0 \times 02
                                       0x02 No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y
Proceeding to upgrade Modules.
Starting Module 1 EPLD Upgrade
Module 1: IO FPGA [Programming]: 100.00% ( 64 of 64 sectors)
Module 1 EPLD upgrade is successful.
Module Type Upgrade-Result
_____
 1 SUP Success
EPLDs upgraded.
Module 1 EPLD upgrade is successful.
```

8. After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

EDID	show version modul	
FLTD	Device	Version
MI	FPGA	0×7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2

Install the RCF on a Cisco Nexus 9336C- FX2 cluster switch

You can install the RCF after setting up the Nexus 9336C-FX2 cluster switch for the first time. You can also use this procedure to upgrade your RCF version on your cluster switch.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are cluster1-01, cluster1-02, cluster1-03, and cluster1-04.
- The cluster LIF names are cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1, and cluster1-04_clus2.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches: network device-discovery show

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
cluster1-0	 1/cdp			
Clustell 0.	_	cs1	Ethernet1/7	N9K-C9336C
	e0d	cs2	Ethernet1/7	N9K-C9336C
cluster1-0	2/cdp			
	e3a	cs1	Ethernet1/8	N9K-C9336C
	e0d	cs2	Ethernet1/8	N9K-C9336C
cluster1-0	3/cdp			
	e3a	cs1	Ethernet1/1/1	N9K-C9336C
	e3b	cs2	Ethernet1/1/1	N9K-C9336C
cluster1-0	4/cdp			
	e3a	cs1	Ethernet1/1/2	N9K-C9336C
	e3b	cs2	Ethernet1/1/2	N9K-C9336C
cluster1::	* >			

- 2. Check the administrative and operational status of each cluster port.
- 3. Verify that all the cluster ports are up with a healthy status: network port show -role cluster

	uster1-01	port show -	LOTE CIT	13 CGI			
Ignore							
Health						Speed (Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e3a false	Cluster	Cluster		up	9000	auto/100000	healthy
	Cluster	Cluster		up	9000	auto/100000	healthy
	uster1-02						
Ignore							
						Speed(Mbps)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

e3a	Cluster	Cluster	up	9000	auto/100000	healthy
false						
e0d	Cluster	Cluster	up	9000	auto/100000	healthy
false						
8 entries	were display	ed.				
Node: clu	ster1-03					
Ignore						
					Speed(Mbps)	Health
Health						
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status						
e3a	Cluster	Cluster	up	9000	auto/100000	healthy
false						
e3b	Cluster	Cluster	up	9000	auto/100000	healthy
false						
Node: clu	ster1-04					
Ignore						
					Speed(Mbps)	Health
Health						
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status						
e0a	Cluster	Cluster	up	9000	auto/100000	healthy
false						
e0b	Cluster	Cluster	up	9000	auto/100000	healthy
false			_			_
cluster1:	:*>					

^{4.} Verify that all the cluster interfaces (LIFs) are on the home port: network interface show -role cluster

	Logical	Status	Network	Current	Current
Is					
Vserver Home	Interface	Admin/Oper	r Address/Mask	Node	Port
Cluster	aluator1-01 alua1	un /un	160 254 2 4/22	aluator1-01	032
true	cluster1-01_clus1	up/up	109.234.3.4/23	Clusteri-01	еза
	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01	e0d
true					
	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02	e3a
true	cluster1-02 clus2	11n/11n	169.254.3.9/23	cluster1-02	eOd
true	01430011 02_01432	αρ/ αρ	103.201.013, 20	0145 0011 02	004
	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03	e3a
true		,			
true	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03	e3b
crue	cluster1-04 clus1	up/up	169.254.1.6/23	cluster1-04	e3a
true	_				
	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04	e3b
true	es were displayed.				

^{5.} Verify that the cluster displays information for both cluster switches: system cluster-switch show -is-monitoring-enabled-operational true

cluster1::*> system cluster-switch show -is-monitoring-enabled-operational true Switch Type Address cluster-network 10.233.205.90 cs1 N9K-C9336C Serial Number: FOCXXXXXXGD Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP cs2 cluster-network 10.233.205.91 N9K-C9336C Serial Number: FOCXXXXXXGS Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP cluster1::*>

6. Disable auto-revert on the cluster LIFs.

cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
false

7. On cluster switch cs2, shut down the ports connected to the cluster ports of the nodes.

```
cs2(config) # interface eth1/1/1-2,eth1/7-8
cs2(config-if-range) # shutdown
```

8. Verify that the cluster LIFs have migrated to the ports hosted on cluster switch cs1. This might take a few seconds:

network interface show -role cluster

	Logical	Status	Network	Current	Current
Is					
Jserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster	cluster1-01 clus1	up/up	169.254.3.4/23	cluster1-01	e3a
true	_				
	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01	e3a
false	cluster1-02 clus1	ıın/ıın	169.254.3.8/23	cluster1-02	e3a
true	01450011 02_01451	αργαρ	103.201.0.0720	Clubtell 02	Cou
	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02	e3a
false	-1+1 02 -11		160 054 1 2/02	-11 02	- 2 -
true	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03	e3a
	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03	e3a
false					
	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04	e3a
true	cluster1-04 clus2	up/up	169.254.1.7/23	cluster1-04	e3a
false	_	1 1			

9. Verify that the cluster is healthy:

cluster show

<pre>cluster1::*> cluster Node</pre>		Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false
4 entries were displa	ayed.		
cluster1::*>			

- 10. Clean the configuration on switch cs2 and perform a basic setup.
 - a. Clean the configuration. This step requires a console connection to the switch.

```
cs2# write erase Warning: This command will erase the startup-configuration. Do you wish to proceed anyway? (y/n) [n] y cs2# reload This command will reboot the system. (y/n)? [n] y cs2#
```

- b. Perform a basic setup of the switch.
- 11. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information about Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

This example shows TFTP being used to copy an RCF to the bootflash on switch cs2.

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

12. Apply the RCF previously downloaded to the bootflash.

For more information about Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

This example shows the RCF file Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt being installed on switch cs2.

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config echo-commands
```

13. Examine the banner output from the show banner moted command. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

```
cs2# show banner motd
*******************
* NetApp Reference Configuration File (RCF)
* Switch : Nexus N9K-C9336C-FX2
* Filename : Nexus 9336C RCF v1.6-Cluster-HA-Breakout.txt
* Date : 10-23-2020
* Version : v1.6
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int e1/1/1-4,
* e1/2/1-4, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int e1/4/1-4,
* e1/5/1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
* Undo breakout commands and return interfaces to 40/100G configuration in
* config mode:
* no interface breakout module 1 port <range> map 10q-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
****************
```

14. Verify that the RCF file is the correct newer version:

show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

- The RCF banner
- The node and port settings
- Customizations

The output varies according to your site configuration. Check the port settings and refer to the release

notes for any changes specific to the RCF that you have installed.

15. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information about Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

```
cs2# copy running-config startup-config
[############################# 100% Copy complete
```

16. Reboot switch cs2. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs2# reload This command will reboot the system. (y/n)? [n] y
```

17. Apply the same RCF and save the running configuration for a second time.

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
cs2# copy running-config startup-config
[################################] 100% Copy complete
```

- 18. Verify the health of cluster ports on the cluster.
 - a. Verify that e0d ports are up and healthy across all nodes in the cluster: network port show -role cluster

								Ignore
.				- ' 1		Speed (Mbps)	Health	Health
Port	IPspace	Broadcast	Domain	Link	MT'U	Admin/Oper	Status	Status
e3a	Cluster	Cluster		up	9000	auto/100000	healthy	false
e3b	Cluster	Cluster		up	9000	auto/100000	healthy	false
Node:	cluster1-0	2						
								Ignore
		_				Speed (Mbps)	Health	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	Status
e3a	Cluster	Cluster	1	up	9000	auto/100000	healthy	false
e3b	Cluster	Cluster	1	up	9000	auto/100000	healthy	false
Node:	cluster1-0	3						
Node:	cluster1-0	3						Ignore
Node:	cluster1-0					Speed(Mbps)	Health	Ignore Health
Node:	cluster1-0	3 Broadcast	Domain	Link	MTU	Speed(Mbps) Admin/Oper	Health Status	_
			Domain	Link up	MTU 		Status	Health
Port	IPspace	Broadcast	Domain			Admin/Oper	Status healthy	Health Status
Port e3a e0d	IPspace Cluster	Broadcast Cluster Cluster	Domain	 up	9000	Admin/Operauto/100000	Status healthy	Health Status false
Port e3a e0d	IPspace Cluster Cluster	Broadcast Cluster Cluster	Domain	 up	9000	Admin/Operauto/100000	Status healthy	Health Status false
Port e3a e0d	IPspace Cluster Cluster cluster	Broadcast Cluster Cluster		up up	9000	Admin/Oper auto/100000 auto/100000	Status healthy healthy	Health Status false false Ignore Health
Port e3a e0d	IPspace Cluster Cluster cluster	Broadcast Cluster Cluster		up up	9000	Admin/Oper auto/100000 auto/100000	Status healthy healthy	Health Status false false Ignore
Port e3a e0d Node:	IPspace Cluster Cluster cluster1-0	Broadcast	Domain	up up Link	9000 9000 MTU	Admin/Oper auto/100000 auto/100000	Status healthy healthy Health Status	Health Status false false Ignore Health Status

b. Verify the switch health from the cluster (this might not show switch cs2, since LIFs are not homed on e0d).

Node/	Local	Discover	red			
					Interface	Platform
cluster1-0						
	_	cs1			Ethernet1/7	N9K-C9336C
		cs2			Ethernet1/7	
cluster01-	2/cdp					
	_	cs1			Ethernet1/8	N9K-C9336C
	e0d	cs2			Ethernet1/8	N9K-C9336C
cluster01-	3/cdp					
	e3a	cs1			Ethernet1/1/1	N9K-C9336C
	e3b	cs2			Ethernet1/1/1	N9K-C9336C
cluster1-0	4/cdp					
	- e3a	cs1			Ethernet1/1/2	N9K-C9336C
	e3b	cs2			Ethernet1/1/2	N9K-C9336C
true	*> syste				monitoring-enabl	ed-operationa
true			Type			ed-operationa Model
true Switch			Туре		monitoring-enabl Address	ed-operationa Model
true Switch cs1			Type clus		monitoring-enabl Address	ed-operationa Model
true Switch cs1 Seria		: FOCXXXX	Type clus		monitoring-enabl Address	ed-operationa Model
true Switch cs1 Seria	l Number	: FOCXXXX	Type clus		monitoring-enabl Address	ed-operationa Model
true Switch cs1 Seria Is M	l Number onitored Reason	: FOCXXXX: true : None : Cisco N	Type clus XXXGD	ter-network	monitoring-enabl Address	ed-operationa Model NX9-C9336
true Switch cs1 Seria Is M Software	l Number onitored Reason Version	: FOCXXXX : true : None : Cisco N 9.3(5)	Type clus XXXGD	ter-network	Address 10.233.205.90	ed-operationa Model NX9-C9336
true Switchcs1 Seria Is M Software Versio	l Number onitored Reason	: FOCXXXX: true : None : Cisco N 9.3(5) : CDP	Type clus XXXGD	ter-network Operating Sy	Address 10.233.205.90 vstem (NX-OS) Sof	Model NX9-C9336
true Switch cs1 Seria Is M Software Versio cs2	l Number onitored Reason Version n Source	: FOCXXXX : true : None : Cisco N 9.3(5) : CDP	Type clus XXXGD Jexus clus	ter-network Operating Sy	Address 10.233.205.90	Model NX9-C9336
true Switch cs1 Seria Is M Software Versio cs2 Seria	l Number onitored Reason Version n Source	: FOCXXXX: true : None : Cisco N 9.3(5) : CDP	Type clus XXXGD Jexus clus	ter-network Operating Sy	Address 10.233.205.90 vstem (NX-OS) Sof	Model NX9-C9336
true Switch cs1 Seria Is M Software Versio cs2 Seria	l Number onitored Reason Version n Source l Number onitored	: FOCXXXX : true : None : Cisco N 9.3(5) : CDP : FOCXXXX	Type clus XXXGD Jexus clus	ter-network Operating Sy	Address 10.233.205.90 vstem (NX-OS) Sof	Model NX9-C9336
true Switchcs1 Seria Is M Software Versio cs2 Seria Is M	l Number onitored Reason Version n Source l Number onitored Reason	: FOCXXXX : true : None : Cisco N 9.3(5) : CDP : FOCXXXX : true : None	Type clus XXXGD Nexus clus XXXGS	ter-network Operating Sy ter-network	Address 10.233.205.90 vstem (NX-OS) Sof	Model NX9-C9336 Ttware, Version
true Switchcs1 Seria Is M Software Versio cs2 Seria Is M	l Number onitored Reason Version n Source l Number onitored Reason	: FOCXXXX : true : None : Cisco N 9.3(5) : CDP : FOCXXXX : true : None : Cisco N	Type clus XXXGD Nexus clus XXXGS	ter-network Operating Sy ter-network	Address 10.233.205.90 vstem (NX-OS) Sof	Model NX9-C9336 Ttware, Version
true Switchcs1 Seria Is M Software Versio cs2 Seria Is M Software	l Number onitored Reason Version n Source l Number onitored Reason	: FOCXXXX : true : None : Cisco N 9.3(5) : CDP : FOCXXXX : true : None : Cisco N 9.3(5)	Type clus XXXGD Nexus clus XXXGS	ter-network Operating Sy ter-network	Address 10.233.205.90 vstem (NX-OS) Sof	Model NX9-C9336 Ttware, Version



You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch.

2020 Nov 17 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Blocking
port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Blocking
port-channel1 on VLAN0092. Inconsistent local vlan.

19. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes. The following example uses the interface example output from step 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

20. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds:

network interface show -role cluster

Current	Logical Is	Status	Network	Current	
	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01	e0d
false true	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01	e0d
false	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02	e0d
true	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02	e0d
false	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03	e3b
true	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03	e3b
false	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04	e3b
true	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04	e3b

21. Verify that the cluster is healthy:

cluster show

```
cluster1::*> cluster show
Node
                Health Eligibility Epsilon
________________
                      true
cluster1-01
                                 false
                true
cluster1-02
                                 false
               true
                      true
cluster1-03
                                 true
               true
                      true
cluster1-04
                                 false
               true
                      true
4 entries were displayed.
cluster1::*>
```

- 22. Repeat Steps 7 to 14 on switch cs1.
- 23. Enable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
True
```

24. Reboot switch cs1. You do this to trigger the cluster LIFs to revert to their home ports. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

```
cs1# reload This command will reboot the system. (y/n)? [n] y
```

25. Verify that the switch ports connected to the cluster ports are up.

```
cs1# show interface brief | grep up
         1
Eth1/1/1
               eth access up
                                                  100G(D)
                               none
Eth1/1/2 1 eth access up
                               none
                                                  100G(D)
       1 eth trunk up
Eth1/7
                                                  100G(D)
                               none
      1 eth trunk up
Eth1/8
                                none
                                                  100G(D)
```

26. Verify that the ISL between cs1 and cs2 is functional:

show port-channel summary

27. Verify that the cluster LIFs have reverted to their home port:

network interface show -role cluster

	_	Status	Network	Current	
Current					
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01	e0d
true	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01	e0d
true	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02	e0d
true	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02	e0d
true	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03	e3b
true	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03	e3b
true	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04	e3b
true	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04	e3b

28. Verify that the cluster is healthy:

cluster show

cluster1-01 true true false cluster1-03 true true true true	Node	Health	Eligibility	Epsilon
cluster1-02 true true false cluster1-03 true true true cluster1-04 true true false				
cluster1-04 true true true false	cluster1-01	true	true	false
cluster1-04 true true false	cluster1-02	true	true	false
	cluster1-03	true	true	true
4 entries were displayed.	cluster1-04	true	true	false
	4 entries were displa	ayed.		

29. Ping the remote cluster interfaces to verify connectivity:

cluster ping-cluster -node local

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03 clus1 169.254.1.3 cluster1-03 e3a
Cluster cluster1-03 clus2 169.254.1.1 cluster1-03 e3b
Cluster cluster1-04 clus1 169.254.1.6 cluster1-04 e3a
Cluster cluster1-04 clus2 169.254.1.7 cluster1-04 e3b
Cluster cluster1-01 clus1 169.254.3.4 cluster1-01 e3a
Cluster cluster1-01 clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02 clus1 169.254.3.8 cluster1-02 e3a
Cluster cluster1-02 clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
. . . . . . . . . . . .
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
......
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
   Local 169.254.1.3 to Remote 169.254.1.7
   Local 169.254.1.3 to Remote 169.254.3.4
   Local 169.254.1.3 to Remote 169.254.3.5
   Local 169.254.1.3 to Remote 169.254.3.8
   Local 169.254.1.3 to Remote 169.254.3.9
   Local 169.254.1.1 to Remote 169.254.1.6
   Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
   Local 169.254.1.1 to Remote 169.254.3.5
   Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Install the RCF on a Cisco Nexus 9336C-FX2 storage switch

The reference configuration files (RCFs) can be upgraded on Cisco Nexus 9336C-FX2 storage switches.

Before you begin

The following conditions must exist before you upgrade the RCF on the storage switch:

• The switch must be fully functioning (there should be no errors in the logs or similar issues).

- You must have checked or set your desired boot variables in the RCF to reflect the desired boot images if
 you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot variables to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco storage upgrade and downgrade procedures. See Cisco Nexus 9000 Series Switches for more information.
- The number of 100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco Ethernet switches page.

Procedure summary

- 1. Check the health status of switches and ports (steps 1-4)
- 2. Download the NX-OS image to Cisco switch st2 and reboot (steps 5-8)
- 3. Copy the RCF to Cisco switch st2 (steps 9-12)
- 4. Recheck the health status of switches and ports (steps 13-15)
- 5. Repeat steps 1-15 for Cisco switch st1.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two storage switches are st1 and st2.
- The nodes are node1 and node2.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all - message MAINT=xh

Where x is the duration of the maintenance window in hours.

2. Check that the storage switches are available:

system switch ethernet show

storage::*> system switch ethernet show Type Address Model Switch st1 storage-network 172.17.227.5 NX9-C9336C Serial Number: FOC221206C2 Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP st2 storage-network 172.17.227.6 NX9-C9336C Serial Number: FOC220443LZ Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP 2 entries were displayed. storage::*>

3. Verify that the node ports are healthy and operational:

storage port show -port-type ENET

				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

4. Check that there are no storage switch or cabling issues with the cluster:

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 5. Download the NX-OS image to switch st2.
- 6. Install the system image so that the new version will be loaded the next time switch st2 is rebooted. The switch will be reboot in 10 seconds with the new image as shown in the following output:

```
st2# install all nxos bootflash:nxos.9.3. 5.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[############### 100% -- SUCCESS
Verifying image type.
[[###############] 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[################ 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[############### 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
                   disruptive
                                      reset default upgrade is not
           yes
hitless
Images will be upgraded according to following table:
Module Image Running-Version(pri:alt)
                                                     New-Version
Upg
Required
-----
1
                                            9.3(3)
                                                         9.3(4)
     nxos
yes
     bios v08.37(01/28/2020):v08.23(09/23/2015)
1
v08.38(05/29/2020) no
Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n] y
input string too long
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.

st2#
```

7. Save the configuration.

You are prompted to reboot the system as shown in the following example:

```
st2# copy running-config startup-config
[#################################] 100% Copy complete.
st2# reload
This command will reboot the system. (y/n)? [n] y
```

8. Confirm that the new NX-OS version number is on the switch.

```
st2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Upgrading a Cisco Nexus 9336C Storage Switch 6
Upgrading a Cisco Nexus 9336C storage switch
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless otherwise stated, there is no warranty, express or implied,
including but not limited to warranties of merchantability and fitness for
a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
Software
BIOS: version 08.38
 NXOS: version 9.3(5)
 BIOS compile time: 05/29/2020
 NXOS image file is: bootflash://nxos.9.3. 5.bin
 NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]
Hardware
 cisco Nexus9000 C9336C Chassis (Nexus 9000 Series)
 Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
 Processor Board ID FOC20291J6K
 Device name: S2
 bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020
           Reason: Reset due to upgrade
   System version: 9.3(5)
   Service:
plugin
   Core Plugin, Ethernet Plugin
   Active Package(s):
st2#
```

9. Copy the RCF on switch st2 to the switch bootflash using one of the following transfer protocols: FTP, HTTP, TFTP, SFTP, or SCP.

For more information about Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

The following example shows HTTP being used to copy an RCF to the bootflash on switch st2:

```
st2# copy http://172.16.10.1//cfg/Nexus 9336C RCF v1.6-Storage.txt
bootflash: vrf management
% Total % Received % Xferd Average Speed Time
                                               Time
                                                     Time
Current
           Upload Total Spent Left
  Dload
Speed
                  100
100
      3254
                          3254 0
                                         0 8175 0 --:--:--
--:--:-
8301
Copy complete, now saving to disk (please wait) ...
Copy complete.
st2#
```

10. Apply the RCF previously downloaded to the bootflash: copy bootflash.

The following example shows the RCF file Nexus_9336C_RCF_v1.6-Storage.txt being installed on switch st2:

```
st2# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-commands
```

11. Verify that the RCF file is the correct newer version:

```
show running-config
```

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

- The RCF banner
- The node and port settings
- Customizations

The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.

Important: In the banner output from the show banner motd command, you must read and follow the instructions in the *IMPORTANT NOTES *section to ensure the proper configuration and operation of the switch.

```
st2# show banner motd
******************
*NetApp Reference Configuration File (RCF)
*Switch: Nexus N9K-C9336C-FX2
*Filename : Nexus 9336C RCF v1.6-Storage.txt
* Date : 10-23-2020
*Version : v1.6
*Port Usage: Storage configuration
*Ports 1-36: 100GbE Controller and Shelf Storage Ports
*IMPORTANT NOTES*
*- This RCF utilizes QoS and requires TCAM re-configuration, requiring RCF
*to be loaded twice with the Storage Switch rebooted in between.
*- Perform the following 4 steps to ensure proper RCF installation:
*(1) Apply RCF first time, expect following messages:
*- Please save config and reload the system...
*- Edge port type (portfast) should only be enabled on ports...
*- TCAM region is not configured for feature QoS class IPv4 ingress...
*(2) Save running-configuration and reboot Cluster Switch
*(3) After reboot, apply same RCF second time and expect following
messages:
*- % Invalid command at '^' marker
*- Syntax error while parsing...
*(4) Save running-configuration again
******************
***
st2#
```

12. After you verify that the software versions and switch settings are correct, copy the running-config file to the startup-config file on switch st2.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

The following example shows the running-config file successfully copied to the startup-config file:

```
st2# copy running-config startup-config
[#############################] 100% Copy complete.
```

13. Recheck that the storage switches are available after the reboot:

system switch ethernet show

storage::*> system switch ethernet show Switch Type Address Model st1 storage-network 172.17.227.5 NX9-C9336C Serial Number: FOC221206C2 Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP st2 storage-network 172.17.227.6 NX9-C9336C Serial Number: FOC220443LZ Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP 2 entries were displayed. storage::*

14. Verify that the switch ports are healthy and operational after the reboot:

storage port show -port-type ENET

				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

15. Recheck that there is no storage switch or cabling issues with the cluster:

system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 16. Repeat this procedure for the RCF on switch st1.
- 17. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Install the RCF on a Cisco Nexus 9336C-FX2 shared switch

From ONTAP 9.9.1, you can use Cisco Nexus 9336C-FX2 switches to combine storage and cluster functionality into a shared switch scenario.

Before you begin

- The cluster switches must be fully functioning (there should be no errors in the logs or similar issues).
- The storage switches must be fully functioning (there should be no errors in the logs or similar issues).
- The names of the two storage switches are *sh1* and *sh2*.
- The example used here loads the shared RCF on to the new switch.

Steps

1. Copy the RCF on switch sh2 to the switch bootflash using one of the following transfer protocols: FTP, HTTP, TFTP, SFTP, or SCP.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

The following example shows HTTP being used to copy an RCF to the bootflash on switch sh2:

```
sh2# copy http://172.16.10.1//cfg/Nexus 9336C RCF v1.7-Cluster-Ha-
Storage.txt bootflash: vrf management
% Total % Received % Xferd
                           Average
                                    Speed Time
                                                 Time
                                                        Time
Current
  Dload
            Upload Total Spent
                                Left
Speed
                                             0
100
       5143
                   100
                            5143
                                    0
                                                  11300
                                                           0 --:--
--:--:-
11300
Copy complete, now saving to disk (please wait) ...
Copy complete.
sh2#
```

2. Apply the RCF previously downloaded to the bootflash: copy bootflash.

The following example shows the RCF file `Nexus_9336C_RCF_v1.7-Cluster-HA-Storage.txt ` being installed on switch sh2:

```
sh2# copy Nexus_9336C_RCF_v1.7-Cluster-HA-Storage.txt running-config echo-commands
```

3. Verify that the RCF file is the correct newer version: show running-config

When you check the output to verify you have the correct RCF, make sure that the following information is correct:

- The RCF banner
- The node and port settings
- Customizations

The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.

Important: In the banner output from the show banner moted command, you must read and follow the instructions in the *IMPORTANT NOTES *section to ensure the proper configuration and operation of the switch.

```
sh2# show banner motd
******************
*NetApp Reference Configuration File (RCF)
*Switch: Nexus N9K-C9336C-FX2
*Filename: Nexus 9336C RCF v1.7-Cluster-HA-Storage.txt
* Date : Jan-08-2021
*Version : v1.7
*Port Usage:
*Ports 1-8: 40/100GbE Intra-Cluster/HA Ports, int e1/1-8
*Port 9: 10GbE breakout Intra-Cluster Ports, int e1/9/1-4
       10: 25GbE breakout Intra-Cluster/HA Ports, int e1/10/1-4
*Ports 11-22: First HA-pair Controller and Shelf Storage Ports, int e1/11-
22
*Ports 23-34: Second HA-pair Controller and Shelf Storage Ports, int
e1/23-34
*Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
* Undo breakout commands and return interfaces to 40/100G configuration in
* config mode:
* no interface breakout module 1 port 9 map 10g-4x
* no interface breakout module 1 port 10 map 25q-4x
* interface Ethernet 1/9-10
* inherit port-profile CLUSTER HA
* priority-flow-control mode auto
* service-policy type qos input HA POLICY
* exit
*IMPORTANT NOTES*
* In certain conditions, N9K-C9336C-FX2 may not be able to auto-negotiate
* speed correctly, and port speed must be manually set, in config mode,
e.g.
* int e1/1
* speed 40000
* int e1/3
* speed 100000
******************
***
sh2#
```

4. After you verify that the software versions and switch settings are correct, copy the running-config

file to the startup-config file on switch sh2.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series NX-OS Command Reference guides.

The following example shows the running-config file successfully copied to the startup-config file:

```
sh2# copy running-config startup-config [############# 100% Copy complete.
```

5. Repeat this procedure for the RCF on switch sh1.

Migrate from a switchless cluster with direct-attached storage by adding two new shared switches

Migrate from a switchless cluster with direct-attached storage

You must be aware of certain configuration information, port connections, and cabling requirements when you migrate a two-node switchless cluster, non-disruptively, to a cluster with Cisco Nexus 9336C-FX2 cluster switches. The procedure you use depends on whether you have two dedicated cluster-network ports on each controller or a single cluster port on each controller. The process documented works for all nodes using optical or Twinax ports but is not supported on this switch if nodes are using onboard 10Gb BASE-T RJ45 ports for the cluster-network ports.

Most systems require two dedicated cluster-network ports on each controller. See Cisco Ethernet Switches for more information.

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using Cisco Nexus 9336C-FX2 switches to enable you to scale beyond two nodes in the cluster.

Before you begin

- Two-node switchless configuration:
 - The two-node switchless configuration must be properly set up and functioning.
 - The nodes must be running ONTAP 9.8 and later.
 - All cluster ports must be in the **up** state.
 - All cluster logical interfaces (LIFs) must be in the **up** state and on their **home** ports.
- Cisco Nexus 9336C-FX2 switch configuration:
 - Both switches must have management network connectivity.
 - There must be console access to the cluster switches.
 - Nexus 9336C-FX2 node-to-node switch and switch-to-switch connections must use Twinax or fiber cables.
 - The NetApp Hardware Universe contains more information about cabling.
 - ∘ Inter-Switch Link (ISL) cables must be connected to ports 1/35 and 1/36 on both 9336C-FX2 switches.
- Initial customization of the 9336C-FX2 switches must be completed. So that the:

- 9336C-FX2 switches are running the latest version of software
- Reference Configuration Files (RCFs) have been applied to the switches
- Any site customization, such as SMTP, SNMP, and SSH must be configured on the new switches.

About this task

The examples in this procedure use the following cluster switch and node nomenclature:

- The names of the 9336C-FX2 switches are cs1 and cs2.
- The names of the cluster SVMs are node1 and node2.
- The names of the LIFs are *node1_clus1* and *node1_clus2* on node 1, and *node2_clus1* and *node2_clus2* on node 2 respectively.
- The cluster1::*> prompt indicates the name of the cluster.
- The cluster ports used in this procedure are *e3a* and *e3b*, as per the AFF A400 controller. The Hardware Universe contains the latest information about the actual cluster ports for your platforms.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh.

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

3. Disable all node-facing ports (not ISL ports) on both the new cluster switches cs1 and cs2. You must not disable the ISL ports.

The following example shows that node-facing ports 1 through 34 are disabled on switch cs1:

```
csl# config
Enter configuration commands, one per line. End with CNTL/Z.
csl(config)# interface e/1-34
csl(config-if-range)# shutdown
```

4. Verify that the ISL and the physical ports on the ISL between the two 9336C-FX2 switches cs1 and cs2 are up on ports 1/35 and 1/36:

```
show port-channel summary
```

The following example shows that the ISL ports are up on switch cs1:

```
csl# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
b - BFD Session Wait
S - Switched R - Routed
U - Up (port-channel)
p - Up in delay-lacp mode (member)
M - Not in use. Min-links not met

-----

Group Port- Type Protocol Member Ports
Channel
------
1 Pol(SU) Eth LACP Eth1/35(P) Eth1/36(P)
```

The following example shows that the ISL ports are up on switch cs2:

```
cs2# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
b - BFD Session Wait
S - Switched R - Routed
U - Up (port-channel)
p - Up in delay-lacp mode (member)
M - Not in use. Min-links not met

-----

Group Port- Type Protocol Member Ports
Channel
------
1 Po1(SU) Eth LACP Eth1/35(P) Eth1/36(P)
```

Display the list of neighboring devices:

show cdp neighbors.

This command provides information about the devices that are connected to the system. The following example lists the neighboring devices on switch cs1:

```
cs1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                 Local Intrfce Hldtme Capability Platform
                                                                Port ID
cs2
                  Eth1/35
                                175
                                      RSIs
                                                 N9K-C9336C
                                                                Eth1/35
cs2
                  Eth1/36
                                175
                                       RSIs
                                                  N9K-C9336C
                                                                Eth1/36
Total entries displayed: 2
```

The following example lists the neighboring devices on switch cs2:

```
cs2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
                 Local Intrfce Hldtme Capability Platform
Device-ID
                                                               Port ID
                 Eth1/35
                               177 RSIS
                                                 N9K-C9336C
                                                               Eth1/35
cs1
                Eth1/36
                               177
                                     RSIs
                                                N9K-C9336C
                                                               Eth1/36
cs1
             )
Total entries displayed: 2
```

6. Verify that all cluster ports are up:

```
network port show - ipspace Cluster
```

Each port should display up for Link and healthy for Health Status:

cluster1::*> network port show -ipspace Cluster								
Node: node	e1							
					Speed(Mbps)	Health		
Port	IPspace	Broadcast Domai	n Link	MTU	Admin/Oper	Status		
e3a	Cluster	Cluster	up	9000	auto/100000	healthy		
e3b	Cluster	Cluster	up	9000	auto/100000	healthy		
Node: node	e2							
					Speed(Mbps)	Health		
Port	IPspace	Broadcast Domai	n Link	MTU	Admin/Oper	Status		
e3a	Cluster	Cluster	up	9000	auto/100000	healthy		
e3b	Cluster	Cluster	up	9000	auto/100000	healthy		
4 entries	were displaye	ed.						

7. Verify that all cluster LIFs are up and operational:

network interface show - vserver Cluster

Each cluster LIF should display true for Is Home and have a Status Admin/Oper of up/up.

cluster1::*	> network in	terface sh	ow -vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Ope	r Address/Mask	Node	Port
Home					
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e3a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e3b
true					
4 entries w	ere displaye	d.			

8. Verify that auto-revert is enabled on all cluster LIFs:

network interface show - vserver Cluster -fields auto-revert

9. Disconnect the cable from cluster port e3a on node1, and then connect e3a to port 1 on cluster switch cs1, using the appropriate cabling supported by the 9336C-FX2 switches.

The NetApp Hardware Universe contains more information about cabling.

- 10. Disconnect the cable from cluster port e3a on node2, and then connect e3a to port 2 on cluster switch cs1, using the appropriate cabling supported by the 9336C-FX2 switches.
- 11. Enable all node-facing ports on cluster switch cs1.

The following example shows that ports 1/1 through 1/34 are enabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# no shutdown
```

12. Verify that all cluster LIFs are **up**, operational, and display as true for Is Home: network interface show - vserver Cluster

The following example shows that all the LIFs are **up** on node1 and node2 and that Is Home results are **true**:

	Logical	Status	Network	Current	Current
Is					
Jserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	nodel_clus1	up/up	169.254.209.69/16	node1	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e3a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e3b
true					

13. Display information about the status of the nodes in the cluster:

cluster show

The following example displays information about the health and eligibility of the nodes in the cluster:

- 14. Disconnect the cable from cluster port e3b on node1, and then connect e3b to port 1 on cluster switch cs2, using the appropriate cabling supported by the 9336C-FX2 switches.
- 15. Disconnect the cable from cluster port e3b on node2, and then connect e3b to port 2 on cluster switch cs2, using the appropriate cabling supported by the 9336C-FX2 switches.
- 16. Enable all node-facing ports on cluster switch cs2.

The following example shows that ports 1/1 through 1/34 are enabled on switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-34
cs2(config-if-range)# no shutdown
```

17. Verify that all cluster ports are up: network port show - ipspace Cluster

The following example shows that all the cluster ports are up on node1 and node2:

cluster1:	:*> network po	ort show -i	.pspace	Clust	ter		
Node: node	e1						
Ignore						Chood (Mana)	IIool+b
Health						Speed(Mbps)	пеатсп
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e3a false	Cluster	Cluster		up	9000	auto/100000	healthy
	Cluster	Cluster		up	9000	auto/100000	healthy
Node: node	= 2						
Ignore							
Health						Speed(Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e3a false	Cluster	Cluster		up	9000	auto/100000	healthy
	Cluster	Cluster		up	9000	auto/100000	healthy
4 entries	were displaye	ed.					

18. Verify that all interfaces display true for Is Home: network interface show - vserver Cluster



This might take several minutes to complete.

The following example shows that all LIFs are **up** on node1 and node2 and that Is Home results are true:

	Logical	Status	Network	Current	Current Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e3a
true		,			
	node2_clus2	up/up	169.254.19.183/16	node2	e3b
true					

19. Verify that both nodes each have one connection to each switch:

show cdp neighbors

The following example shows the appropriate results for both switches:

```
cs1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                                  Port ID
node1
                  Eth1/1
                                 133
                                       Η
                                                    AFFA400
                                                                  e3a
node2
                  Eth1/2
                                 133
                                       Н
                                                    AFFA400
                                                                  еЗа
cs2
                  Eth1/35
                                       RSIs
                                                    N9K-C9336C
                                                                  Eth1/35
                                 175
cs2
                  Eth1/36
                                 175
                                        RSIs
                                                    N9K-C9336C
                                                                  Eth1/36
Total entries displayed: 4
cs2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                                  Port ID
node1
                  Eth1/1
                                                                  e3b
                                 133
                                        Η
                                                    AFFA400
node2
                  Eth1/2
                                 133
                                                    AFFA400
                                                                  e3b
                                        Η
cs1
                  Eth1/35
                                 175
                                        RSIs
                                                    N9K-C9336C
                                                                  Eth1/35
                  Eth1/36
                                        RSIs
                                                                  Eth1/36
cs1
                                 175
                                                    N9K-C9336C
Total entries displayed: 4
```

20. Display information about the discovered network devices in your cluster: network device-discovery show -protocol cdp

lode/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e3a	cs1	0/2	N9K-C9336C
	e3b	cs2	0/2	N9K-C9336C
node1	/cdp			
	e3a	cs1	0/1	N9K-C9336C
	e3b	cs2	0/1	N9K-C9336C

21. Verify that the storage configuration of HA pair 1 (and HA pair 2) is correct and error free: system switch ethernet show

storage::*> system switch ethernet show Switch Address Model sh1 storage-network 172.17.227.5 C9336C Serial Number: FOC221206C2 Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP sh2 storage-network 172.17.227.6 C9336C Serial Number: FOC220443LZ Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP 2 entries were displayed. storage::*>

22. Verify that the settings are disabled:

network options switchless-cluster show



It might take several minutes for the command to complete. Wait for the '3-minute lifetime to expire' announcement.

The false output in the following example shows that the configuration settings are disabled:

cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false

23. Verify the status of the node members in the cluster:

cluster show

The following example shows information about the health and eligibility of the nodes in the cluster:

24. Ensure that the cluster network has full connectivity:

cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e3a
Cluster node1 clus2 169.254.49.125 node1 e3b
Cluster node2 clus1 169.254.47.194 node2 e3a
Cluster node2 clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

25. Change the privilege level back to admin:

```
set -privilege admin
```

- 26. Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands:
 - ° system switch ethernet log setup-password
 - ° system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```

Setup the shared switch

The examples in this procedure use the following switch and node nomenclature:

- The names of the two shared switches are sh1 and sh2.
- The nodes are node1 and node2.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands, ONTAP commands are used unless otherwise indicated.

Steps

1. Verify that the storage configuration of HA pair 1 (and HA pair 2) is correct and error free: system switch ethernet show

storage::*> system switch ethernet show

Switch Type Address Model -----

sh1

storage-network 172.17.227.5 C9336C

Serial Number: FOC221206C2

Is Monitored: true Reason: None

Software Version: Cisco Nexus Operating System (NX-OS) Software,

Version

9.3(5)

Version Source: CDP

sh2

storage-network 172.17.227.6 C9336C

Serial Number: FOC220443LZ

Is Monitored: true Reason: None

Software Version: Cisco Nexus Operating System (NX-OS) Software,

Version

9.3(5)

Version Source: CDP 2 entries were displayed.

storage::*>

2. Verify that the storage node ports are healthy and operational:

storage port show -port-type ENET

storage	e::*> st	orage p	ort show -po	ort-type ENET			
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	100	enabled	online	30
	e5a	ENET	storage	100	enabled	online	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	100	enabled	online	30
	e5a	ENET	storage	100	enabled	online	30
	e5b	ENET	storage	100	enabled	online	30

- 3. Move the HA pair 1, NSM224 path A ports to sh1 port range 11-22.
- 4. Install a cable from HA pair 1, node1, path A to sh1 port range 11-22. For example, the path A storage port on an AFF A400 is e0c.
- 5. Install a cable from HA pair 1, node2, path A to sh1 port range 11-22.
- 6. Verify that the node ports are healthy and operational: storage port show -port-type ENET

				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
 node1							
noder	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

7. Check that there are no storage switch or cabling issues with the cluster:

system health alert show -instance

storage::*> system health alert show -instance
There are no entries matching your query.

- 8. Move the HA pair 1, NSM224 path B ports to sh2 port range 11-22.
- 9. Install a cable from HA pair 1, node1, path B to sh2 port range 11-22. For example, the path B storage port on an AFF A400 is e5b.
- 10. Install a cable from HA pair 1, node2, path B to sh2 port range 11-22.
- 11. Verify that the node ports are healthy and operational:

storage port show -port-type ENET

storage	e::*> st	orage p	ort show -	port-type ENET			
				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

12. Verify that the storage configuration of HA pair 1 is correct and error free: system switch ethernet show

Switch	Type	Address	Model
sh1			
	storage-network	172.17.227.5	C9336C
Serial Number:	FOC221206C2		
Is Monitored:	true		
Reason:	None		
Software Version:	Cisco Nexus Operating Sy	stem (NX-OS) Softwa	are,
Version			
	9.3(5)		
Version Source:	CDP		
sh2			
	storage-network	172.17.227.6	C9336C
Corial Number.	FOC220443LZ		
serrar number:			
Is Monitored:	true		
Is Monitored: Reason:		stem (NX-OS) Softwa	are,
Is Monitored: Reason:	None	stem (NX-OS) Softwa	are,
Is Monitored: Reason: Software Version:	None	stem (NX-OS) Softwa	are,
Is Monitored: Reason: Software Version:	None Cisco Nexus Operating Sy 9.3(5)	stem (NX-OS) Softwa	are,

13. Reconfigure the unused (controller) secondary storage ports on HA pair 1 from storage to networking. If more than one NS224 was direct attached, there will be ports that should be reconfigured.

```
storage port modify -node [node name] -port [port name] -mode network
```

To place storage ports into a broadcast domain:

- network port broadcast-domain create (to create a new domain, if needed)
- network port broadcast-domain add-ports (to add ports to an existing domain)
- 14. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Migrate from a switched configuration with direct-attached storage by adding two new shared switches

Migrate from a switched configuration with direct-attached storage

You must be aware of certain configuration information, port connections, and cabling requirements when you are replacing some older Cisco Nexus cluster switches with Cisco Nexus 9336C-FX2 shared switches.

- · The following switches are supported:
 - Nexus 9336C-FX2
 - Nexus 3232C
- The switches use the following ports for connections to nodes:
- Nexus 9336C-FX2:
 - Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int e1/1/1-4, e1/2/1-4, e1/3/1-4
 - Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int e1/4/1-4, e1/5/1-4, e1/6/1-4
 - Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
- Nexus 3232C:
 - Ports 1-30: 10/40/100 GbE
- The switches use the following Inter-Switch Link (ISL) ports:
 - Ports int e1/35-36: Nexus 9336C-FX2
 - Ports e1/31-32: Nexus 3232C
- The Hardware Universe contains information about supported cabling for all cluster switches.

See Hardware Universe for more information.

- You have configured some of the ports on Nexus 9336C-FX2 switches to run at 100 GbE.
- You have planned, migrated, and documented 100 GbE connectivity from nodes to Nexus 9336C-FX2 switches.
- The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page. See Cisco Ethernet switches.

 You can migrate nondisruptively other Cisco cluster switches from an ONTAP cluster to Cisco Nexus 9336C-FX2 network switches.

Before you begin

- The existing switch network must be properly set up and functioning.
- All ports must be in the **up** state to ensure nondisruptive operations.
- The Nexus 9336C-FX2 switches must be configured and operating under the proper version of NX-OS installed and reference configuration file (RCF) applied.
- The existing network configuration must have the following:
 - A redundant and fully functional NetApp cluster using both older Cisco switches.
 - Management connectivity and console access to both the older Cisco switches and the new switches.
 - All cluster LIFs in the **up** state with the cluster LIFs are on their home ports.
 - $_{\circ}$ ISL ports enabled and cabled between the other Cisco switches and between the new switches.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The existing Cisco Nexus 3232C cluster switches are c1 and c2.
- The new Nexus 9336C-FX2 switches are sh1 and sh2.
- The nodes are node1 and node2.
- The cluster LIFs are *node1_clus1* and *node1_clus2* on node 1, and *node2_clus1* and *node2_clus2* on node 2 respectively.
- Switch c2 is replaced by switch sh2 first and then switch c1 is replaced by switch sh1.

Steps

 If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=x h
```

Where x is the duration of the maintenance window in hours.

- 2. Check the administrative and operational status of each cluster port.
- 3. Verify that all the cluster ports are up with a healthy status:

```
network port show -role cluster
```

cluster		ork port show -rc	le clu	ıster		
					Speed(Mbps) Health	Ignore Health
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Ope Status	
e3a	Cluster	Cluster	up	9000	auto/100000 healthy	false
e3b	Cluster	Cluster	up	9000	auto/100000 healthy	false
Node: r	node2					
					Speed(Mbps) Health	Ignore Health
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper Status	Status
e3a	Cluster	Cluster	up	9000	auto/100000 healthy	false
e3b	Cluster	Cluster	up	9000	auto/100000 healthy	false
4 entri cluster	es were di	splayed.				

4. Verify that all the cluster interfaces (LIFs) are on the home port: network interface show -role cluster

cluster1	l::*> network	interface s	show -role cluster			
	Logical	Status	Network	Current	Current	Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	Home
Cluster						
	node1_clus1	up/up	169.254.3.4/23	node1	e3a	true
	node1_clus2	up/up	169.254.3.5/23	node1	e3b	true
	node2_clus1	up/up	169.254.3.8/23	node2	e3a	true
	node2_clus2	up/up	169.254.3.9/23	node2	e3b	true
4 entri	es were displa	ayed.				
cluster1	1::*>					

5. Verify that the cluster displays information for both cluster switches: system cluster-switch show -is-monitoring-enabled-operational true

cluster1::*> system cluster-switch show -is-monitoring-enabled-operational true Switch Type Address cluster-network 10.233.205.90 sh1 N9K-C9336C Serial Number: FOCXXXXXXGD Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP sh2 cluster-network 10.233.205.91 N9K-C9336C Serial Number: FOCXXXXXXGS Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP cluster1::*>

6. Disable auto-revert on the cluster LIFs.

cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
false

7. Shutdown the c2 switch:

c2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c2(config)# interface ethernet <int range>
c2(config)#shutdown

8. Verify that the cluster LIFs have migrated to the ports hosted on cluster switch sh1:

network interface show -role cluster This might take a few seconds.

```
cluster1::*> network interface show -role cluster
       Logical Status Network Current
                                                    Current Is
Vserver Interface Admin/Oper Address/Mask Node
                                                    Port
Cluster
       node1_clus1 up/up 169.254.3.4/23 node1 e3a
true
        node1 clus2 up/up 169.254.3.5/23 node1
                                                   e3a
false
        node2 clus1 up/up 169.254.3.8/23 node2
                                                    e3a
true
        node2 clus2 up/up 169.254.3.9/23 node2
                                                   e3a
false
4 entries were displayed.
cluster1::*>
```

- 9. Replace switch c2 with the new switch sh2 and re-cable the new switch.
- 10. Verify that the ports are back up on sh2. **Note** that the LIFs are still on switch c1.
- 11. Shutdown the c1 switch:

```
c1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c1(config)# interface ethernet <int range>
c1(config)#shutdown
```

12. Verify that the cluster LIFs have migrated to the ports hosted on cluster switch sh2. This might take a few seconds.

```
cluster1::*> network interface show -role cluster
            Status Network Current Is
     Logical
Vserver Interface Admin/Oper Address/Mask Node Port
                                              Home
Cluster
     node1_clus1 up/up 169.254.3.4/23 node1 e3a true
     node1 clus2 up/up
                       169.254.3.5/23 node1
                                         e3a
                                              false
      node2_clus1 up/up
                       169.254.3.8/23 node2 e3a
                                              true
                       169.254.3.9/23 node2
                                              false
      node2 clus2 up/up
                                         e3a
4 entries were displayed.
cluster1::*>
```

13. Replace switch c1 with the new switch sh1 and re-cable the new switch.

- 14. Verify that the ports are back up on sh1. **Note** that the LIFs are still on switch c2.
- 15. Enable auto-revert on the cluster LIFs:

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
True
```

16. Verify that the cluster is healthy:

cluster show

Migrate from a switchless configuration with switchattached storage by reusing the storage switches

Migrate the storage switches

By reusing the storage switches the storage switches of HA pair 1 become the shared switches. **Cabling diagram for switch-attached**



Steps

1. Verify that the storage configuration of HA pair 1 (and HA pair 2) is correct and error free: system switch ethernet show

storage::*> system switch ethernet show

Switch Type Address Model

sh1

storage-network 172.17.227.5 C9336C

Serial Number: FOC221206C2

Is Monitored: true
Reason: none

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

9.3(5)

Version Source: CDP

sh2

storage-network 172.17.227.6 C9336C

Serial Number: FOC220443LZ

Is Monitored: true
Reason: None

Software Version: Cisco Nexus Operating System (NX-OS) Software, Version

9.3(5)

Version Source: CDP 2 entries were displayed.

storage::*>

2. Verify that the node ports are healthy and operational:

storage port show -port-type ENET

storage::*> storage port show -port				Speed			VLAN	
Node	Port	Type	Mode	(Gb/s)	State	Status	ID	
node1								
	e0c	ENET	storage	100	enabled	online	30	
	e0d	ENET	storage	100	enabled	online	30	
	e5a	ENET	storage	100	enabled	online	30	
	e5b	ENET	storage	100	enabled	online	30	
node2								
	e0c	ENET	storage	100	enabled	online	30	
	e0d	ENET	storage	100	enabled	online	30	
	e5a	ENET	storage	100	enabled	online	30	
	e5b	ENET	storage	100	enabled	online	30	

3. Move the HA pair 1, NSM224 path A cables from storage switch A to the shared NS224 storage ports for

HA pair 1, path A on storage switch A.

- 4. Move the cable from HA pair 1, node A, path A to the shared storage port for HA pair 1, node A on storage switch A.
- 5. Move the cable from HA pair 1, node B, path A to the shared storage port for HA pair 1, node B on storage switch A.
- 6. Verify the storage attached to HA pair 1, storage switch A is healthy: system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 7. Replace the storage RCF on shared switch A with the shared RCF file. See Install the RCF on a Cisco Nexus 9336C-FX2 shared switch for further details.
- 8. Verify the storage attached to HA pair 1, storage switch B is healthy: system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 9. Move the HA pair 1, NSM224 path B cables from storage switch B to the shared NS224 storage ports for HA pair 1, path B to storage switch B.
- 10. Move the cable from HA pair 1, node A, path B to the shared storage port for HA pair 1, node A, path B on storage switch B.
- 11. Move the cable from HA pair 1, node B, path B to the shared storage port for HA pair 1, node B, path B on storage switch B.
- 12. Verify the storage attached to HA pair 1, storage switch B is healthy: system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 13. Replace the storage RCF file on shared switch B with the shared RCF file. See Install the RCF on a Cisco Nexus 9336C-FX2 shared switch for further details.
- 14. Verify the storage attached to HA pair 1, storage switch B is healthy: system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

15. Install the ISLs between shared switch A and shared switch B:

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config) # interface e1/35-36
sh1 (config-if-range) # no lldp transmit
sh1 (config-if-range) # no lldp receive
sh1 (config-if-range) # switchport mode trunk
sh1 (config-if-range) # no spanning-tree bpduguard enable
sh1 (config-if-range) # channel-group 101 mode active
sh1 (config-if-range) # exit
sh1 (config) # interface port-channel 101
sh1 (config-if) # switchport mode trunk
sh1 (config-if) # spanning-tree port type network
sh1 (config-if) # exit
sh1 (config) # exit
```

- Convert HA pair 1 from a switchless cluster to a switched cluster. Use the cluster port assignments
 defined by the shared RCF. See Install NX-OS software and Reference Configuration Files (RCFs) for
 further details.
- 17. Verify that the switched networking configuration is valid: network port show

Migrate from a switched cluster with switch-attached storage by reusing the storage switches

Migrate the storage switches

By reusing the storage switches the storage switches of HA pair 1 become the shared switches. **Cabling diagram for switch-attached**

Switch Attached



Steps

1. Verify that the storage configuration of HA pair 1 (and HA pair 2) is correct and error free: system switch ethernet show

storage::*> system switch ethernet show Address Model Switch storage-network 172.17.227.5 C9336C Serial Number: FOC221206C2 Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP sh2 storage-network 172.17.227.6 C9336C Serial Number: FOC220443LZ Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP 2 entries were displayed. storage::*>

- 2. Move the HA pair 1, NSM224 path A cables from storage switch A to the NSM224 storage ports for HA pair 1, path A on storage switch A.
- 3. Move the cable from HA pair 1, node A, path A to the NSM224 storage port for HA pair 1, node A on storage switch A.
- 4. Move the cable from HA pair 1, node B, path A to the NSM224 storage port for HA pair 1, node B on storage switch A.
- 5. Verify the storage attached to HA pair 1, storage switch A is healthy: storage port show -port-type ENET

				Speed				VLAN
Node	Port	Type	Mode	(Gb/s)		State	Status	ID
node1								
	e0c	ENET	storage		100	enabled	online	30
	e0d	ENET	storage		100	enabled	online	30
	e5a	ENET	storage		100	enabled	online	30
	e5b	ENET	storage		100	enabled	online	30
node2								
	e0c	ENET	storage		100	enabled	online	30
	e0d	ENET	storage		100	enabled	online	30
	e5a	ENET	storage		100	enabled	online	30
	e5b	ENET	storage		100	enabled	online	30

- 6. Replace the storage RCF on shared switch A with the shared RCF file. See Install the RCF on a Cisco Nexus 9336C-FX2 shared switch for further details.
- 7. Verify the storage attached to HA pair 1, storage switch A is healthy: system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 8. Move the HA pair 1, NSM224 path B cables from storage switch B to the shared NS224 storage ports for HA pair 1, path B to storage switch B.
- 9. Move the cable from HA pair 1, node A, path B to the shared storage port for HA pair 1, node A, path B on storage switch B.
- 10. Move the cable from HA pair 1, node B, path B to the shared storage port for HA pair 1, node B, path B on storage switch B.
- 11. Verify the storage attached to HA pair 1, storage switch B is healthy: system health alert show -instance

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

- 12. Replace the storage RCF file on shared switch B with the shared RCF file. See Install the RCF on a Cisco Nexus 9336C-FX2 shared switch for further details.
- 13. Verify the storage attached to HA pair 1, storage switch B is healthy: system health alert show -instance

storage::*> system health alert show -instance
There are no entries matching your query.

14. Verify the storage configuration of HA pair 1 is correct and error free:

system switch ethernet show

storage::*> system switch ethernet show Address Model Switch Type storage-network 172.17.227.5 C9336C Serial Number: FOC221206C2 Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP sh2 storage-network 172.17.227.6 C9336C Serial Number: FOC220443LZ Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5)Version Source: CDP 2 entries were displayed. storage::*>

15. Install the ISLs between shared switch A and shared switch B:

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# interface e1/35-36
sh1 (config-if-range)# no lldp transmit
sh1 (config-if-range)# no lldp receive
sh1 (config-if-range)# switchport mode trunk
sh1 (config-if-range)# no spanning-tree bpduguard enable
sh1 (config-if-range)# channel-group 101 mode active
sh1 (config-if-range)# exit
sh1 (config)# interface port-channel 101
sh1 (config-if)# switchport mode trunk
sh1 (config-if)# spanning-tree port type network
sh1 (config-if)# exit
sh1 (config)# exit
```

- 16. Migrate the cluster networking from the existing cluster switches to the shared switches using the switch replacement procedure and the shared RCF. The new shared switch A is "cs1". The new shared switch B is "cs2". See Replace a Cisco Nexus 9336C-FX2 shared switch and Install the RCF on a Cisco Nexus 9336C-FX2 shared switch for further details.
- 17. Verify that the switched networking config is valid: network port show
- 18. Remove the unused cluster switches.
- 19. Remove the unused storage switches.

Replace a Cisco Nexus 9336C-FX2 shared switch

Replace a Cisco Nexus 9336C-FX2 shared switch

Replacing a defective Nexus 9336C-FX2 shared switch is a nondisruptive procedure (NDU).

Before you begin

The following conditions must exist before performing the switch replacement in the current environment and on the replacement switch.

- Existing cluster and network infrastructure:
 - The existing cluster must be verified as completely functional, with at least one fully connected cluster switch.
 - All cluster ports must be **up**.
 - All cluster logical interfaces (LIFs) must be **up** and on their home ports.
 - The ONTAP cluster ping-cluster -node node1 command must indicate that basic connectivity and larger than PMTU communication are successful on all paths.
- Nexus 9336C-FX2 replacement switch:
 - Management network connectivity on the replacement switch must be functional.
 - Console access to the replacement switch must be in place.

- The node connections are ports 1/1 through 1/34:
- All Inter-Switch Link (ISL) ports must be disabled on ports 1/35 and 1/36.
- The desired reference configuration file (RCF) and NX-OS operating system image switch must be loaded onto the switch.
- Any previous site customizations, such as STP, SNMP, and SSH, should be copied to the new switch.

About this task

You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.

The examples in this procedure use the following switch and node nomenclature:

- The names of the existing Nexus 9336C-FX2 switches are sh1 and sh2.
- The name of the new Nexus 9336C-FX2 switches are newsh1 and newsh2.
- The node names are *node1* and *node2*.
- The cluster ports on each node are named e3a and e3b.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The prompt for changes to all cluster nodes is cluster1::*>.



The following procedure is based on the following network topology:

<pre>cluster1::*> network port show -ipspace Cluster</pre>										
Node: node1										
Ignore						Speed(Mbps)	Uool+h			
Health						speed (MDPS)	nealth			
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status			
Status										
	Cluster	Cluster		up	9000	auto/100000	healthy			
false	Cluster	Cluster		un	9000	auto/100000	hoalthu			
false	CIUSCEI	Clustel		ир	3000	auto/100000	nearchy			
Node: nod	le?									
Node: 1100										
Ignore										
Health						Speed(Mbps)	Health			
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status			
Status										

e3a							
	Cluster	(Cluster	ир	9000	auto/100000	healthv
false				- 1			1
e3b	Cluster	(Cluster	up	9000	auto/100000	healthy
false				_			_
4 entries	s were dis	splayed	d.				
cluster1:				ow -vserve	c Clust		
_	Logica	al S	Status	Network		Current	Current
Is	T		. 1 . / 0	7.1.1 /26	1	27. 1	5
Vserver	Interi	ace <i>E</i>	Aamın/Oper	Address/M	ask	Noae	Port
Home							
Cluster							
	node1	clus1	up/up	169.254.2	09.69/1	6 node1	e3a
true	_	_					
	node1_	clus2	up/up	169.254.4	9.125/1	6 node1	e3b
true							
	node2_	_clus1	up/up	169.254.4	7.194/1	6 node2	e3a
true							
	1 0		,		/ .		a 21a
	node2_	_clus2	up/up	169.254.1	9.183/1	6 node2	e3b
true	node2_	_clus2	up/up	169.254.1	9.183/1	6 node2	esp
	node2_ s were dis	_		169.254.1	9.183/1	6 node2	esp
4 entries	s were dis	splayed	d.				esp
4 entries cluster1:	s were dis	splayed ork dev	d. vice-disco	169.254.1			esp
4 entries cluster1:	s were dis ::*> netwo	splayed ork dev	d. vice-disco overed	very show	-protoc	ol cdp	
4 entries cluster1:	s were dis ::*> netwo	splayed ork dev	d. vice-disco overed		-protoc	ol cdp	Platform
4 entries cluster1: Node/	s were dis ::*> netwo	splayed ork dev	d. vice-disco overed	very show	-protoc	ol cdp	
4 entries cluster1: Node/ Protocol	s were dis ::*> netwo Local Port	splayed ork dev	d. vice-disco overed	very show	-protoc	ol cdp	
4 entries cluster1: Node/ Protocol	s were dis ::*> netwo Local Port /cdp	splayed ork dev Disco Devic	d. vice-disco overed	very show	-protoc Inter	ol cdp face	Platform
4 entries cluster1: Node/ Protocol	s were dis ::*> netwo Local Port /cdp e3a	splayed ork dev Disco Device sh1	d. vice-disco overed	very show	-protoc Inter Eth1/	ol cdp face 	Platform N9K-C9336C
4 entries cluster1: Node/ Protocol	s were dis ::*> netwo Local Port /cdp	splayed ork dev Disco Device sh1	d. vice-disco overed	very show	-protoc Inter	ol cdp face 	Platform
4 entries cluster1: Node/ Protocol node2	s were dis ::*> netwo Local Port /cdp e3a e3b	splayed ork dev Disco Device sh1	d. vice-disco overed	very show	-protoc Inter Eth1/	ol cdp face 	Platform N9K-C9336C
4 entries cluster1: Node/ Protocol node2	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp	splayed ork dev Disco Device sh1	d. vice-disco overed	very show	-protoc Inter Eth1/	ol cdp face 2 2 2	Platform N9K-C9336C
4 entries cluster1: Node/ Protocol node2	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp	splayed ork dev Disco Devic sh1 sh2	d. vice-disco overed	very show	-protoc Inter Eth1/ Eth1/	ol cdp face 2 2	Platform N9K-C9336C N9K-C9336C
4 entries cluster1: Node/ Protocol node2	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp e3a	splayed ork dev Disco Device sh1 sh2	d. vice-disco	very show	-protoc Inter Eth1/ Eth1/	ol cdp face 2 2	Platform N9K-C9336C N9K-C9336C
4 entries cluster1: Node/ Protocol node2	s were dis ::*> netwo Local Port/cdp e3a e3b /cdp e3a e3b	splayed ork dev Disco Device sh1 sh2	d. vice-disco	very show	-protoc Inter Eth1/ Eth1/	ol cdp face 2 2	Platform N9K-C9336C N9K-C9336C
4 entries cluster1: Node/ Protocol node2 node1 4 entries	s were dis ::*> netwo Local Port/cdp e3a e3b /cdp e3a e3b	splayed ork dev Disco Device sh1 sh2 sh1 sh2	d. vice-disco	very show	-protoc Inter Eth1/ Eth1/	ol cdp face 2 2	Platform N9K-C9336C N9K-C9336C
4 entries cluster1: Node/ Protocol node2 node1 4 entries sh1# show	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp e3a e3b s were dis	splayed Disco Device sh1 sh2 sh1 sh2 splayed	d. vice-disco overed ce (LLDP:	very show	-protoc Inter Eth1/ Eth1/ Eth1/	ol cdp face 2 2	Platform N9K-C9336C N9K-C9336C N9K-C9336C N9K-C9336C
4 entries cluster1: Node/ Protocol node2 node1 4 entries sh1# show	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp e3a e3b s were dis	splayed Disco Device sh1 sh2 sh1 sh2 splayed splayed shbors R - Ro	d. vice-disco overed ce (LLDP:	very show (ChassisID)	-protoc Inter Eth1/ Eth1/ Eth1/ Eth1/	ol cdp face 2 2 1	Platform N9K-C9336C N9K-C9336C N9K-C9336C N9K-C9336C
4 entries cluster1: Node/ Protocol node2 node1 4 entries sh1# show	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp e3a e3b s were dis w cdp neighty Codes:	splayed Disco Device sh1 sh2 sh1 sh2 splayed ghbors R - Ro S - Sv	d. vice-disco overed ce (LLDP: d. outer, T - vitch, H -	very show ChassisID) Trans-Bride Host, I -	-protoc Inter Eth1/ Eth1/ Eth1/ dge, B IGMP,	ol cdp face 2 2 1 1 1	Platform N9K-C9336C N9K-C9336C N9K-C9336C N9K-C9336C
cluster1: Node/ Protocol node2 node1 4 entries sh1# show	s were dis ::*> netwo Local Port /cdp e3a e3b /cdp e3a e3b s were dis w cdp neighty Codes:	splayed Disco Device Sh1 Sh2 Sh1 Sh2 Splayed Shbors R - Ro S - Sw V - Vo S - Si	d. vice-disco overed ce (LLDP: vitch, H - oIP-Phone, upports-ST	Trans-Briden Host, I - D - Remote P-Dispute	-protoc Inter Eth1/ Eth1/ Eth1/ dge, B IGMP, ely-Man	ol cdp face 2 2 1 1 - Source-Rou r - Repeater	Platform N9K-C9336C N9K-C9336C N9K-C9336C N9K-C9336C

node1	Eth1/1	144	Н	FAS2980	e3a					
node2	Eth1/2	145	Н	FAS2980	e3a					
sh2	Eth1/35	176	RSIS	N9K-C9336C	Eth1/35					
sh2 (FDO220329V5)	Eth1/36	176	RSIs	N9K-C9336C	Eth1/36					
Total entries disp	layed: 4									
sh2# show cdp neig	hbors									
Capability Codes:	R - Router, T -	Trans-	Bridge, B -	Source-Route-B	ridge					
	S - Switch, H -	Host,	I - IGMP, r	- Repeater,						
	V - VoIP-Phone,	D - Re	motely-Manag	ed-Device,						
	s - Supports-STP-Dispute									
Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID					
node1	Eth1/1	139	Н	FAS2980	eb					
node2	Eth1/2	124	Н	FAS2980	eb					
sh1	Eth1/35	178	RSIS	N9K-C9336C	Eth1/35					
sh1	Eth1/36	178	RSIS	N9K-C9336C	Eth1/36					
Total entries disp	layed: 4									

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node \star -type all -message MAINT=xh
```

Where x is the duration of the maintenance window in hours.

- 2. Optional: Install the appropriate RCF and image on the switch, newsh2, and make any necessary site preparations.
 - a. If necessary, verify, download, and install the appropriate versions of the RCF and NX-OS software for the new switch. If you have verified that the new switch is correctly set up and does not need updates to the RCF and NX-OS software, continue to Step 3.
 - b. Go to the NetApp Cluster and Management Network Switches Reference Configuration File Description Page on the NetApp Support Site.
 - c. Click the link for the Cluster Network and Management Network Compatibility Matrix, and then note the required switch software version.
 - d. Click your browser's back arrow to return to the Description page, click CONTINUE, accept the license agreement, and then go to the Download page.
 - e. Follow the steps on the Download page to download the correct RCF and NX-OS files for the version of ONTAP software you are installing.
- 3. On the new switch, log in as admin and shut down all the ports that will be connected to the node cluster interfaces (ports 1/1 to 1/34).
 - If the switch that you are replacing is not functional and is powered down, go to Step 4. The LIFs on the cluster nodes should have already failed over to the other cluster port for each node.

```
newsh2# config
Enter configuration commands, one per line. End with CNTL/Z.
newsh2(config)# interface e1/1-34
newsh2(config-if-range)# shutdown
```

4. Verify that all cluster LIFs have auto-revert enabled.

network interface show - vserver Cluster -fields auto-revert

5. Verify that all the cluster LIFs can communicate: cluster ping-cluster <node name>

```
cluster1::*> cluster ping-cluster node1
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e3a
Cluster node1 clus2 169.254.49.125 node1 e3b
Cluster node2 clus1 169.254.47.194 node2 e3a
Cluster node2 clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Shut down the ISL ports 1/35 and 1/36 on the Nexus 9336C-FX2 switch sh1.

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1(config)# interface e1/35-36
sh1(config-if-range)# shutdown
sh1(config-if-range)#
```

- 7. Remove all the cables from the Nexus 9336C-FX2 sh2 switch, and then connect them to the same ports on the Nexus C9336C-FX2 newsh2 switch.
- 8. Bring up the ISLs ports 1/35 and 1/36 between the sh1 and newsh2 switches, and then verify the port channel operation status.

Port-Channel should indicate Po1(SU) and Member Ports should indicate Eth1/35(P) and Eth1/36(P).

This example enables ISL ports 1/35 and 1/36 and displays the port channel summary on switch sh1.

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config) # int e1/35-36
sh1 (config-if-range) # no shutdown
sh1 (config-if-range) # show port-channel summary
                 P - Up in port-channel (members)
Flags: D - Down
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/35(P) Eth1/36(P)
sh1 (config-if-range)#
```

9. Verify that port e3b is up on all nodes:

network port show ipspace Cluster

The output should be like the following:

cluster1:	:*> network po	ort show -ipspace	Clus	ter		
Node: node	e1					
Ignore					Speed(Mbps)	Uool+h
Health					speed (MDPs)	nearch
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status						
e3a	Cluster	Cluster	up	9000	auto/100000	healthy
false						
e3b false	Cluster	Cluster	up	9000	auto/100000	healthy
Idise						
Node: node	=2					
Ignore						
ignore					Speed (Mbps)	Health
Health						
	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status						
	Cluster	Cluster	up	9000	auto/100000	healthy
false e3b	Cluster	Cluster	110	9000	auto/auto	_
false	OI US CCI	CIUSCCI	αр	2000	4407440	
4 entries were displayed.						

10. On the same node you used in the previous step, revert the cluster LIF associated with the port in the previous step by using the network interface revert command.

In this example, LIF node1_clus2 on node1 is successfully reverted if the Home value is true and the port is e3b.

The following commands return LIF node1_clus2 on node1 to home port e3a and displays information about the LIFs on both nodes. Bringing up the first node is successful if the Is Home column is **true** for both cluster interfaces and they show the correct port assignments, in this example e3a and e3b on node1.

cluster1::*	> network int	erface show	-vserver Cluster		
	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	nodel_clus1	up/up	169.254.209.69/16	node1	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					
	node2 clus1	up/up	169.254.47.194/16	node2	e3a
true	_				
	node2 clus2	up/up	169.254.19.183/16	node2	e3a
false	_				
4 entries we	ere displayed				
	1 2				

11. Display information about the nodes in a cluster:

cluster show

This example shows that the node health for node1 and node2 in this cluster is true:

12. Verify that all physical cluster ports are up:

network port show ipspace Cluster

cluster1:	:*> network	port show -ipspace	Clust	er		
Node node	1					
Ignore						
					Speed(Mbps)	Health
Health						
	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status						
e3a	Cluster	Cluster	up	9000	auto/100000	healthy
false			ı		·	1
e3b	Cluster	Cluster	up	9000	auto/100000	healthy
false						
27 1						
Node: nod	le2					
Ignore						
5					Speed (Mbps)	Health
Health						
Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status						
- 2 -	G1	G1		0000		h 1 + h
e3a false	Cluster	Cluster	up	9000	auto/100000	healthy
	Cluster	Cluster	up	9000	auto/100000	healthy
false	0140 001	0140001	αp	3000	4450/100000	rear city
	were displa	yed.				
	-	-				

13. Verify that all the cluster LIFs can communicate:

cluster ping-cluster

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e3a
Cluster node1 clus2 169.254.49.125 node1 e3b
Cluster node2 clus1 169.254.47.194 node2 e3a
Cluster node2 clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

14. Confirm the following cluster network configuration: network port show

Ts					Speed	d (Mbps	5)	Health
Status e3a Cluster Cluster up 9000 auto/100000 healthy false e3b Cluster Cluster up 9000 auto/100000 healthy false 4 entries were displayed. Cluster1::*> network interface show -vserver Cluster Logical Status Network Current Cur Is Vserver Interface Admin/Oper Address/Mask Node Por Home		Pspace	Broadcas	st Domain	Link	МТП	Admin/Oper	Status
### Cluster Cluster up 9000 auto/100000 healthy false e3b		110000	Diodaodi	o Domain		1110	riamilii, oper	Scacas
false e3b Cluster Cluster up 9000 auto/100000 healthy false 4 entries were displayed. Cluster1::*> network interface show -vserver Cluster Logical Status Network Current Cur Is Vserver Interface Admin/Oper Address/Mask Node Por Home Cluster node1_clus1 up/up 169.254.209.69/16 node1 e3s true node1_clus2 up/up 169.254.49.125/16 node1 e3s true node2_clus1 up/up 169.254.47.194/16 node2 e3s true node2_clus2 up/up 169.254.19.183/16 node2 e3s true 4 entries were displayed. Cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor								
false e3b Cluster Cluster up 9000 auto/100000 healthy false 4 entries were displayed. Cluster1::*> network interface show -vserver Cluster Logical Status Network Current Cur Is Vserver Interface Admin/Oper Address/Mask Node Por Home Cluster nodel_clus1 up/up 169.254.209.69/16 node1 e3s true nodel_clus2 up/up 169.254.49.125/16 node1 e3s true node2_clus1 up/up 169.254.47.194/16 node2 e3s true node2_clus2 up/up 169.254.19.183/16 node2 e3s true 4 entries were displayed. Cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor								
e3b Cluster Cluster up 9000 auto/100000 healthy false 4 entries were displayed. cluster1::*> network interface show -vserver Cluster Logical Status Network Current Cur Is Vserver Interface Admin/Oper Address/Mask Node Por Home Cluster node1_clus1 up/up 169.254.209.69/16 node1 e3a true node2_clus1 up/up 169.254.49.125/16 node1 e3a true node2_clus1 up/up 169.254.47.194/16 node2 e3a true node2_clus2 up/up 169.254.19.183/16 node2 e3a true 10 node2_clus2 up/up 169.254.19.183/16 node2 e3a true 11 node2_clus2 up/up 169.254.19.183/16 node2 e3a true 12 node2_clus2 up/up 169.254.19.183/16 node2 e3a true 13 node2_clus2 up/up 169.254.19.183/16 node2 e3a true 14 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	3a C	Cluster	Cluster		up	9000	auto/100000	healthy
false 4 entries were displayed. cluster1::*> network interface show -vserver Cluster	alse							
d entries were displayed. cluster1::*> network interface show -vserver Cluster Logical Status Network Current Curs Is Vserver Interface Admin/Oper Address/Mask Node Por Home Cluster node1_clus1 up/up 169.254.209.69/16 node1 e3s true node2_clus2 up/up 169.254.49.125/16 node1 e3s true node2_clus1 up/up 169.254.47.194/16 node2 e3s true node2_clus2 up/up 169.254.19.183/16 node2 e3s true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	3b C	Cluster	Cluster		up	9000	auto/100000	healthy
cluster1::*> network interface show -vserver Cluster Logical Status Network Current Cur Is Vserver Interface Admin/Oper Address/Mask Node Por Home Cluster node1_clus1 up/up 169.254.209.69/16 node1 e3s true node1_clus2 up/up 169.254.49.125/16 node1 e3s true node2_clus1 up/up 169.254.47.194/16 node2 e3s true node2_clus2 up/up 169.254.19.183/16 node2 e3s true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	alse							
Logical Status Network Current Current S	entries w	ere displ	layed.					
Is Vserver Interface Admin/Oper Address/Mask Node Por Home	luster1::*	> network	x interface	show -vse	erver	Clust	ter	
Vserver Interface Admin/Oper Address/Mask Node Por Home		Logical	Status	Netwo	rk		Current	Current
Home Cluster node1_clus1 up/up 169.254.209.69/16 node1 e3a true node1_clus2 up/up 169.254.49.125/16 node1 e3a true node2_clus1 up/up 169.254.47.194/16 node2 e3a true node2_clus2 up/up 169.254.19.183/16 node2 e3a true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	S							
Cluster node1_clus1 up/up 169.254.209.69/16 node1 e3strue node1_clus2 up/up 169.254.49.125/16 node1 e3strue node2_clus1 up/up 169.254.47.194/16 node2 e3strue node2_clus2 up/up 169.254.19.183/16 node2 e3strue 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	server	Interfac	ce Admin/Op	per Addres	ss/Mas	sk	Node	Port
node1_clus1 up/up 169.254.209.69/16 node1 e3strue node1_clus2 up/up 169.254.49.125/16 node1 e3strue node2_clus1 up/up 169.254.47.194/16 node2 e3strue node2_clus2 up/up 169.254.19.183/16 node2 e3strue 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	ome							
node1_clus1 up/up 169.254.209.69/16 node1 e3strue node1_clus2 up/up 169.254.49.125/16 node1 e3strue node2_clus1 up/up 169.254.47.194/16 node2 e3strue node2_clus2 up/up 169.254.19.183/16 node2 e3strue 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor								
node1_clus1 up/up 169.254.209.69/16 node1 e3strue node1_clus2 up/up 169.254.49.125/16 node1 e3strue node2_clus1 up/up 169.254.47.194/16 node2 e3strue node2_clus2 up/up 169.254.19.183/16 node2 e3strue 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor								
true node1_clus2 up/up 169.254.49.125/16 node1 e3k true node2_clus1 up/up 169.254.47.194/16 node2 e3k true node2_clus2 up/up 169.254.19.183/16 node2 e3k true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	luster							
node1_clus2 up/up 169.254.49.125/16 node1 e3k true node2_clus1 up/up 169.254.47.194/16 node2 e3k true node2_clus2 up/up 169.254.19.183/16 node2 e3k true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor		node1_cl	lus1 up/up	169.25	54.209	9.69/1	l6 node1	e3a
true node2_clus1 up/up 169.254.47.194/16 node2 e3s true node2_clus2 up/up 169.254.19.183/16 node2 e3s true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	rue					/ .		
node2_clus1 up/up 169.254.47.194/16 node2 e38 true node2_clus2 up/up 169.254.19.183/16 node2 e38 true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor		nodel_cl	lus2 up/up	169.25	54.49	.125/1	l6 nodel	e3b
true node2_clus2 up/up 169.254.19.183/16 node2 e3k true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	rue	1 0 1	1 /	1.60.01	- 4 4 7	104/	1.6	2
node2_clus2 up/up 169.254.19.183/16 node2 e3k true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor		nodez_ci	lusi up/up	169.23	04.4/	.194/_	lb nodez	esa
true 4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	rue	nodo? al	1102 110/110	160 20	5/ 10	102/1	le nodo?	o 2 h
4 entries were displayed. cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	X110	nodez_ci	lusz up/up	109.23	34.19	.103/-	rodez	esp
cluster1::> network device-discovery show -protocol cdp Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor		oro displ	arrod					
Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor node2 /cdp e3a sh1 0/2 N9K-C9336C e3b newsh2 0/2 N9K-C93 node1 /cdp	entiles w	rere dispi	layeu.					
Node/ Local Discovered Protocol Port Device (LLDP: ChassisID) Interface Platfor	luster1::>	→ network	device-disc	roverv sho	_m - w.	rotoco	ol cdp	
Protocol Port Device (LLDP: ChassisID) Interface Platfor					J. P.		or oab	
	·			: Chassis	sID)	Inte	cface	Platform
e3a sh1 0/2 N9K-C9336C e3b newsh2 0/2 N9K-C93 node1 /cdp								
e3a sh1 0/2 N9K-C9336C e3b newsh2 0/2 N9K-C93 node1 /cdp								
e3b newsh2 0/2 N9K-C93	ode2	/cdp						
nodel /cdp		e3a s	sh1 0/2		1	N9K-C9	9336C	
		e3b r	newsh2			0/2		N9K-C9336C
e3a sh1 0/1 N9K-C93	ode1	/cdp						
		e3a s	sh1			0/1		N9K-C9336C
e3b newsh2 0/1 N9K-C93		e3b r	newsh2			0/1		N9K-C9336C
4 entries were displayed.	entrice	ere displ	laved.					

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                    Local Intrfce Hldtme Capability Platform
                                                                   Port
ID
node1
                    Eth1/1
                                   144
                                          Η
                                                      FAS2980
                                                                   e3a
node2
                    Eth1/2
                                   145
                                                      FAS2980
                                                                   e3a
                                         Η
newsh2
                    Eth1/35
                                   176
                                          RSIs
                                                      N9K-C9336C
Eth1/35
newsh2
                    Eth1/36
                                   176
                                          RSIs
                                                     N9K-C9336C
Eth1/36
Total entries displayed: 4
sh2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater,
                 V - VoIP-Phone, D - Remotely-Managed-Device,
                 s - Supports-STP-Dispute
Device-ID
                  Local Intrfce Hldtme Capability Platform
                                                                 Port ID
node1
                  Eth1/1
                                 139
                                                    FAS2980
                                                                 e3b
                                       Η
node2
                  Eth1/2
                                 124
                                                    FAS2980
                                                                 eb
                                        Н
sh1
                  Eth1/35
                                 178
                                        RSIs
                                                    N9K-C9336C
                                                                 Eth1/35
                  Eth1/36
sh1
                                 178
                                        RSIs
                                                    N9K-C9336C
                                                                 Eth1/36
Total entries displayed: 4
```

^{15.} Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the following commands:

[°] system switch ethernet log setup password

[°] system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sh1
sh2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: sh1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: sh2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the cluster?
y|n: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

- 16. Move the storage ports from the old switch sh2 to the new switch newsh2.
- 17. Verify the storage attached to HA pair 1, shared switch newsh2 is healthy.
- 18. Verify the storage attached to HA pair 2, shared switch newsh2 is healthy: storage port show -port-type ENET

				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

19. Verify that the shelves are correctly cabled:

storage shelf port show -fields remote- device, remote-port

- 20. Remove the old switch sh2.
- 21. Repeat these steps for the switch sh1 and new switch newsh1.
- 22. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=END

Cisco Nexus 92300YC switches

Cisco Nexus 92300YC switch overview

If you want to build ONTAP clusters with more than two nodes, you need two supported cluster network switches. You can use additional management switches, which are optional.

You can install the Cisco Nexus 92300YC switch (X190003/R) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following table lists the part number and description for the 92300YC switch, fans, and power supplies:

Part number	Description
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX (PTSX = Port Side Exhaust)
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN (PSIN = Port Side Intake)
X-NXA-FAN-35CFM-B	Fan, Cisco N9K port side intake airflow
X-NXA-FAN-35CFM-F	Fan, Cisco N9K port side exhaust airflow
X-NXA-PAC-650W-B	Power supply, Cisco 650W - port side intake
X-NXA-PAC-650W-F	Power supply, Cisco 650W - port side exhaust

Cisco Nexus 92300YC switch airflow details:

- Port-side exhaust airflow (standard air) --Cool air enters the chassis through the fan and power supply
 modules in the cold aisle and exhausts through the port end of the chassis in the hot aisle. Port-side
 exhaust airflow with blue coloring.
- Port-side intake airflow (reverse air) --Cool air enters the chassis through the port end in the cold aisle and exhausts through the fan and power supply modules in the hot aisle. Port-side intake airflow with burgundy coloring.

Other supported Switches

Nexus 3232C

You can install the Cisco Nexus 3232C switch (X190100) NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

Nexus 3132Q-V

You can install the Cisco Nexus 3132Q-V switch (X190001) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following cluster switches are no longer available from NetApp, but will be supported by Cisco for a limited time:

Nexus 5596UP/5596T

You can install the Cisco Nexus 5596UP switch (X1967-R6) or 5596T (X1989-R6) in a NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

The Nexus 5596UP switch also supports one or two 16-port expansion modules (X1988-R6).

The Nexus 5596T switch is only supported as a cluster interconnect switch for the FAS2520 and is intended to be used for performing nondisruptive hardware upgrades.

End of Availability details.

Available documentation

The following table lists the documentation available for the Cisco Nexus 92300YC switches.

Title	Description
Setup the Cisco® Nexus 92300YC cluster switches	Describes how to setup and configure your Cisco Nexus 92300YC cluster switches.
Install NX-OS and Reference Configuration Files (RCFs)	Describes how to install NX-OS and reference configuration files (RCFs) on Nexus 92300YC cluster switch.
Configure a new Cisco Nexus 92300YC Switch	Describes how to migrate from environments that use older Cisco switches to environments that use Cisco 92300YC switches.
Migrate from an older Cisco Switch to a Cisco Nexus 92300YC Switch	Describes the procedure to replace an older Cisco switch with a Cisco Nexus 92300YC cluster switch.
Migrate from a two-node Switchless Cluster	Describes how to migrate from a two-node switchless cluster environment to a two-node switched environment using Cisco Nexus 92300YC cluster switches.
Replace a Cisco Nexus 92300YC Cluster Switch	Describes the procedure to replace a defective Cisco Nexus 92300YC switch in a cluster and download the switch operating system and reference configuration file.

Set up

Set up the switches

If you do not already have the required configuration information and documentation, you

need to gather that information before setting up your cluster and management network switches.

- You must have access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- You must have the required cluster network and management network switch documentation.

See Required documentation for more information.

• You must have the required controller documentation and ONTAP documentation.

NetApp documentation

- You must have the applicable licenses, network and configuration information, and cables.
- · You must have the completed cabling worksheets.



Due to the complexity that can result from illustrating layers of cabling, this guide does not provide cabling graphics. This guide does provide sample worksheets with recommended port assignments and blank worksheets that you can use to set up your cluster.



For more information refer to the Hardware Universe.

 All Cisco cluster network and management network switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software but do not have the RCFs loaded.



You must download the applicable NetApp cluster network and management network RCFs from the NetApp Support Site at mysupport.netapp.com for the switches that you receive.

 In addition, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for the 92300YC cluster switches. See Installing the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches for details.

Steps

1. Rack the cluster network and management network switches and controllers.

If you are installing your	Then
Cisco Nexus 9336C-FX2 in a NetApp system cabinet	See the <i>Installing a Cisco Nexus</i> 9336C-FX2 cluster switch and pass-through panel in a NetApp cabinet guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3232C in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.

If you are installing your	Then
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.
Cisco Nexus 5596UP/5596T in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 5596 cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.

- 2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheets.
- 3. Power on the cluster network and management network switches and controllers.
- 4. Perform an initial configuration of the cluster network switches based on information provided in Required configuration information.
- 5. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
- 6. Check the version on the cluster network switches, and if necessary, download the NetApp-supported version of the software to the switches.
 - If you download the NetApp-supported version of the software, then you must also download the *NetApp Cluster Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and the instructions from the Cisco Ethernet Switches page.
- 7. Check the software version on the network switches and, if necessary, download the NetApp-supported version of the software to the switches. If you have your own switches, refer to the Cisco site.

If you download the NetApp-supported version of the software, then you must also download the *NetApp Management Network Switch Reference Configuration File* and merge it with the configuration you saved in Step 5. You can download the file and instructions from the Cisco Ethernet Switches page.

Related information

Required cluster configuration information

Required documentation

Sample and blank cabling worksheets

Required cluster configuration information

To configure your cluster, you need the appropriate number and type of cables and cable connectors for your switches. Depending on the type of switch you are initially configuring, you need to connect to the switch console port with the included console cable; you also need to provide specific network information.

Required network information for all switches

You need the following network information for all switch configurations:

- · IP subnet for management network traffic
- · Host names and IP addresses for each of the storage system controllers and all applicable switches

 Most storage system controllers are managed through the e0M interface by connecting to the Ethernet service port (wrench icon). On AFF A800 and AFF A700 systems, the e0M interface uses a dedicated Ethernet port.

Refer to the Hardware Universe for latest information.

Required network information for Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches

For the Cisco Nexus 9336C-FX2, 92300YC, 3232C, 3132Q-V, and 5596UP/5596T switches, you need to provide applicable responses to the following initial setup questions when you first boot the switch. Your site's security policy defines the responses and services to enable.

Abort Auto Provisioning and continue with normal setup? (yes/no)

Respond with yes. The default is no.

• Do you want to enforce secure password standard? (yes/no)

Respond with yes. The default is yes.

• Enter the password for admin:

The default password is "admin"; you must create a new, strong password. A weak password can be rejected.

Would you like to enter the basic configuration dialog? (yes/no)

Respond with **yes** at the initial configuration of the switch.

Create another login account? (yes/no)

Your answer depends on your site's policies on alternate administrators. The default is **no**.

Configure read-only SNMP community string? (yes/no)

Respond with no. The default is no.

Configure read-write SNMP community string? (yes/no)

Respond with **no**. The default is no.

• Enter the switch name.

The switch name is limited to 63 alphanumeric characters.

Continue with Out-of-band (mgmt0) management configuration? (yes/no)

Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip address.

Configure the default-gateway? (yes/no)

Respond with yes. At the IPv4 address of the default-gateway: prompt, enter your default gateway.

• Configure advanced IP options? (yes/no)

Respond with no. The default is no.

• Enable the telnet service? (yes/no)

Respond with no. The default is no.

• Enabled SSH service? (yes/no)

Respond with yes. The default is yes.



SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.

- Enter the type of SSH key you want to generate (dsa/rsa/rsa1). The default is rsa.
- Enter the number of key bits (1024-2048).
- Configure the NTP server? (yes/no)

Respond with no. The default is no.

• Configure default interface layer (L3/L2):

Respond with L2. The default is L2.

Configure default switch port interface state (shut/noshut):

Respond with **noshut**. The default is noshut.

• Configure CoPP system profile (strict/moderate/lenient/dense):

Respond with strict. The default is strict.

Would you like to edit the configuration? (yes/no)

You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.

• Use this configuration and save it? (yes/no)

Respond with **yes** to save the configuration. This automatically updates the kickstart and system images.



If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

For more information about the initial configuration of your switch, see the following guides:

Cisco Nexus 9336C-FX2 Installation and Upgrade Guides

Cisco Nexus 92300YC Installation and Upgrade Guides

Cisco Nexus 5000 Series Hardware Installation Guide

Cisco Nexus 3000 Series Hardware Installation Guide

Install the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches

You can use this procedure to install the applicable configuration file for cluster switch health monitoring of Nexus 92300YC cluster switches. In ONTAP releases 9.5P7 and earlier and 9.6P2 and earlier, you must download the cluster switch health monitor configuration file separately. In ONTAP releases 9.5P8 and later, 9.6P3 and later, and 9.7 and later, the cluster switch health monitor configuration file is bundled with ONTAP.

Before you setup the switch health monitor for 92300YC cluster switches, you must ensure that the ONTAP cluster is up and running.



It is advisable to enable SSH in order to use all features available in CSHM.

- 1. Download the cluster switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the NetApp Software download page.
 - a. On the Software download page, select Switch Health Monitor Configuration Files
 - b. Select Platform = **ONTAP** and click **Go!**
 - c. On the Switch Health Monitor Configuration Files for ONTAP page, click View & Download
 - d. On the Switch Health Monitor Configuration Files for ONTAP Description page, click **Download** for the applicable cluster switch model, for example: **Cisco Nexus 92300YC**
 - e. On the End User License Agreement page, click Accept
 - f. On the Switch Health Monitor Configuration Files for ONTAP Download page, select the applicable configuration file, for example, Cisco_Nexus_92300YC.zip
- 2. Upload the applicable zip file to your internal web server where the IP address is X.X.X.X.

For an internal web server IP address of 192.168.2.20 and assuming a /usr/download directory exists, you can upload your zip file to your web server using scp:

```
% scp Cisco_Nexus_92300YC.zip admin@192.168.2.20:/usr/download/Cisco_Nexus_92300YC.zip
```

3. Access the advanced mode setting from one of the ONTAP systems in the cluster, using the command setprivilege advanced:

```
cluster1::> set -privilege advanced
```

4. Run the switch health monitor configure command system cluster-switch configure-health-monitor -node * -package-url X.X.X.X/location_to_download_zip_file:

```
cluster1::> system cluster-switch configure-health-monitor -node *
-package-url 192.168.2.20/usr/download/Cisco_Nexus_92300YC.zip
```

5. Verify that the command output contains the text string "downloaded package processed successfully". If

an error occurs, contact NetApp support.

6. Run the command system cluster-switch show on the ONTAP system and ensure that the cluster switches are discovered with the monitored field set to "True".

cluster1::> system cluster-switch show



If at any time you revert to an earlier version of ONTAP, you will need to install the CSHM configuration file again to enable switch health monitoring of 92300YC cluster switches.

Required documentation

You need specific switch and controller documentation to set up your ONTAP cluster.

Required documentation for cluster network switches

To set up the Cisco Nexus 9336C-FX2 and 92300YC switches, you need the following documentation from the Cisco Nexus 9000 Series Switches Support page:

Document title	Description
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.

Document title	Description
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

To set up the Cisco Nexus 3232C and 3132Q-V switches, you need the following documentation from the Cisco Nexus 3000 Series Switches Support page:

Document title	Description
Nexus 3000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 3000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 3000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 3000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.
Nexus 3000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 3000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 3000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 3000 series switches.

To set up the Cisco Nexus 5596 switch, you need the following documents from Cisco Nexus 5000 Series Switches Support page:

Document title	Description
Nexus 5000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 5000 Series Switch Software Configuration Guide (choose the guide for the software you are using)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide	Provides information about how to downgrade the switch to the supported ONTAP switch software, if necessary.
Cisco Nexus 5000 Series NX-OS Command Reference Master Index	Provides an alphabetical list of all the commands supported for a specific NX-OS release.
Cisco Nexus 5000 and Nexus 2000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 5000 switches.
Nexus 5000 Series NX-OS System Message Reference	Describes troubleshooting information.
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000 Series, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 5000 series switches.

Required documentation for supported ONTAP systems

To set up an ONTAP system, you need the following documents for your version of the operating system from the ONTAP 9 Documentation Center.

Name	Description
Controller-specific Installation and Setup Instructions	Describes how to install NetApp hardware.
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.
Hardware Universe	Provides NetApp hardware configuration and compatibility information.

Rail kit and cabinet documentation

To install a Cisco switch in a NetApp cabinet, see the following hardware documentation:

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet	Describes how to install a Cisco Nexus 3232C switch in a four-post NetApp cabinet.
Installing a Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 3132Q-V switch in a four-post NetApp cabinet.
Installing a Cisco Nexus 5596 switch and pass-through panel in a NetApp Cabinet	Describes how to install a Cisco Nexus 5596 switch in a NetApp cabinet.

Considerations for using Smart Call Home

Smart Call Home monitors the hardware and software components on your network, to generate an email-based notification of critical system conditions. When an event occurs on your device, Smart Call Home raises an alert to all the recipients that are configured in your destination profile.

You must configure a cluster network switch to communicate using email with the Smart Call Home system. You can optionally set up your cluster network switch to take advantage of Cisco's embedded Smart Call Home support feature.

Before you can use Smart Call Home feature, you need to be aware of the following considerations:

- An email server must be in place.
- The switch must have IP connectivity to the email server.
- The contact name (SNMP server contact), phone number, and street address information must be configured.
- This is required to determine the origin of messages received.
- A CCO ID must be associated with an appropriate Cisco SMARTnet Service contract for your company.
- Cisco SMARTnet Service must be in place for the device to be registered.

The Cisco support site contains information about the commands to configure Smart Call Home.

Cisco support site

Sample and blank cabling worksheets

Cisco Nexus 9336C-FX2 cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10GbE node 1	1	4x10GbE node 1
2	4x10GbE node 2	2	4x10GbE node 2
3	4x10GbE node 3	3	4x10GbE node 3
4	4x25GbE node 4	4	4x25GbE node 4
5	4x25GbE node 5	5	4x25GbE node 5
6	4x25GbE node 6	6	4x25GbE node 6
7	4x100GbE node 7	7	4x100GbE node 7
8	4x100GbE node 8	8	4x100GbE node 8
9	4x100GbE node 9	9	4x100GbE node 9
10	4x100GbE node 10	10	4x100GbE node 10
11	4x100GbE node 11	11	4x100GbE node 11
12	4x100GbE node 12	12	4x100GbE node 12
13	4x100GbE node 13	13	4x100GbE node 13
14	4x100GbE node 14	14	4x100GbE node 14
15	4x100GbE node 15	15	4x100GbE node 15
16	4x100GbE node 16	16	4x100GbE node 16
17	4x100GbE node 17	17	4x100GbE node 17
18	4x100GbE node 18	18	4x100GbE node 18
19	4x100GbE node 19	19	4x100GbE node 19
20	4x100GbE node 20	20	4x100GbE node 20

Cluster switch A		Cluster switch B	
21	4x100GbE node 21	21	4x100GbE node 21
22	4x100GbE node 22	22	4x100GbE node 22
23	4x100GbE node 23	23	4x100GbE node 23
24	4x100GbE node 24	24	4x100GbE node 24
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A	Cluster switch B	
1	1	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
10	10	

Cluster switch A		Cluster switch B	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 34	Reserved	25 through 34	Reserved
35	100G ISL to switch B port 35	35	100G ISL to switch A port 35
36	100G ISL to switch B port 36	36	100G ISL to switch A port 36

Cisco Nexus 92300YC cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	10/25 GbE node	1	10/25 GbE node
2	10/25 GbE node	2	10/25 GbE node
3	10/25 GbE node	3	10/25 GbE node
4	10/25 GbE node	4	10/25 GbE node
5	10/25 GbE node	5	10/25 GbE node
6	10/25 GbE node	6	10/25 GbE node
7	10/25 GbE node	7	10/25 GbE node
8	10/25 GbE node	8	10/25 GbE node
9	10/25 GbE node	9	10/25 GbE node
10	10/25 GbE node	10	10/25 GbE node
11	10/25 GbE node	11	10/25 GbE node
12	10/25 GbE node	12	10/25 GbE node
13	10/25 GbE node	13	10/25 GbE node
14	10/25 GbE node	14	10/25 GbE node
15	10/25 GbE node	15	10/25 GbE node
16	10/25 GbE node	16	10/25 GbE node
17	10/25 GbE node	17	10/25 GbE node
18	10/25 GbE node	18	10/25 GbE node
19	10/25 GbE node	19	10/25 GbE node
20	10/25 GbE node	20	10/25 GbE node
21	10/25 GbE node	21	10/25 GbE node

Cluster switch A		Cluster switch B	
22	10/25 GbE node	22	10/25 GbE node
23	10/25 GbE node	23	10/25 GbE node
24	10/25 GbE node	24	10/25 GbE node
25	10/25 GbE node	25	10/25 GbE node
26	10/25 GbE node	26	10/25 GbE node
27	10/25 GbE node	27	10/25 GbE node
28	10/25 GbE node	28	10/25 GbE node
29	10/25 GbE node	29	10/25 GbE node
30	10/25 GbE node	30	10/25 GbE node
31	10/25 GbE node	31	10/25 GbE node
32	10/25 GbE node	32	10/25 GbE node
33	10/25 GbE node	33	10/25 GbE node
34	10/25 GbE node	34	10/25 GbE node
35	10/25 GbE node	35	10/25 GbE node
36	10/25 GbE node	36	10/25 GbE node
37	10/25 GbE node	37	10/25 GbE node
38	10/25 GbE node	38	10/25 GbE node
39	10/25 GbE node	39	10/25 GbE node
40	10/25 GbE node	40	10/25 GbE node
41	10/25 GbE node	41	10/25 GbE node
42	10/25 GbE node	42	10/25 GbE node
43	10/25 GbE node	43	10/25 GbE node

Cluster switch A		Cluster switch B	Cluster switch B	
44	10/25 GbE node	44	10/25 GbE node	
45	10/25 GbE node	45	10/25 GbE node	
46	10/25 GbE node	46	10/25 GbE node	
47	10/25 GbE node	47	10/25 GbE node	
48	10/25 GbE node	48	10/25 GbE node	
49	40/100 GbE node	49	40/100 GbE node	
50	40/100 GbE node	50	40/100 GbE node	
51	40/100 GbE node	51	40/100 GbE node	
52	40/100 GbE node	52	40/100 GbE node	
53	40/100 GbE node	53	40/100 GbE node	
54	40/100 GbE node	54	40/100 GbE node	
55	40/100 GbE node	55	40/100 GbE node	
56	40/100 GbE node	56	40/100 GbE node	
57	40/100 GbE node	57	40/100 GbE node	
58	40/100 GbE node	58	40/100 GbE node	
59	40/100 GbE node	59	40/100 GbE node	
60	40/100 GbE node	60	40/100 GbE node	
61	40/100 GbE node	61	40/100 GbE node	
62	40/100 GbE node	62	40/100 GbE node	
63	40/100 GbE node	63	40/100 GbE node	
64	40/100 GbE node	64	40/100 GbE node	

Cluster switch A		Cluster switch B	
65	100 GbE ISL to switch B port 65	65	100 GbE ISL to switch A port 65
66	100 GbE ISL to switch B port 66	66	100 GbE ISL to switch A port 65

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	

Cluster switch A	Cluster switch B	
16	16	
17	17	
18	18	
19	19	
20	20	
21	21	
22	22	
23	23	
24	24	
25	25	
26	26	
27	27	
28	28	
29	29	
30	30	
31	31	
32	32	
33	33	
34	34	
35	35	
36	36	
37	37	

Cluster switch A	Cluster switch B	
38	38	
39	39	
40	40	
41	41	
42	42	
43	43	
44	44	
45	45	
46	46	
47	47	
48	48	
49	49	
50	50	
51	51	
52	52	
53	53	
54	54	
55	55	
56	56	
57	57	
58	58	
59	59	

Cluster switch A		Cluster switch B	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL to switch B port 65	65	ISL to switch A port 65
66	ISL to switch B port 66	66	ISL to switch A port 66

Cisco Nexus 3232C cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide. Each switch can be configured as a single 100GbE, 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G/100G node	1	4x10G/40G/100G node
2	4x10G/40G/100G node	2	4x10G/40G/100G node
3	4x10G/40G/100G node	3	4x10G/40G/100G node
4	4x10G/40G/100G node	4	4x10G/40G/100G node
5	4x10G/40G/100G node	5	4x10G/40G/100G node
6	4x10G/40G/100Gnode	6	4x10G/40G/100Gnode
7	4x10G/40G/100G node	7	4x10G/40G/100G node
8	4x10G/40G/100G node	8	4x10G/40G/100G node
9	4x10G/40G/100G node	9	4x10G/40G/100G node

Cluster switch A		Cluster switch B	
10	4x10G/40G/100G node	10	4x10G/40G/100G node
11	4x10G/40G/100G node	11	4x10G/40G/100G node
12	4x10G/40G/100G node	12	4x10G/40G/100G node
13	4x10G/40G/100G node	13	4x10G/40G/100G node
14	4x10G/40G/100G node	14	4x10G/40G/100G node
15	4x10G/40G/100G node	15	4x10G/40G/100G node
16	4x10G/40G/100G node	16	4x10G/40G/100G node
17	4x10G/40G/100G node	17	4x10G/40G/100G node
18	4x10G/40G/100G node	18	4x10G/40G/100G node
19	40G/100G node 19	19	40G/100G node 19
20	40G/100G node 20	20	40G/100G node 20
21	40G/100G node 21	21	40G/100G node 21
22	40G/100G node 22	22	40G/100G node 22
23	40G/100G node 23	23	40G/100G node 23
24	40G/100G node 24	24	40G/100G node 24
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage	
1		1		
2		2		
3		3		
4		4		
5		5		
6		6		
7		7		
8		8		
9		9		
10		10		
11		11		
12		12		
13		13		
14		14		
15		15		
16		16		
17		17		
18		18		
19		19		
20		20		
21		21		

Cluster switch A		Cluster switch B	
22		22	
23		23	
24		24	
25 through 30	Reserved	25 through 30	Reserved
31	100G ISL to switch B port 31	31	100G ISL to switch A port 31
32	100G ISL to switch B port 32	32	100G ISL to switch A port 32

Cisco Nexus 3132Q-V cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide. Each switch can be configured as a single 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G node	1	4x10G/40G node
2	4x10G/40G node	2	4x10G/40G node
3	4x10G/40G node	3	4x10G/40G node
4	4x10G/40G node	4	4x10G/40G node
5	4x10G/40G node	5	4x10G/40G node
6	4x10G/40G node	6	4x10G/40G node
7	4x10G/40G node	7	4x10G/40G node
8	4x10G/40G node	8	4x10G/40G node
9	4x10G/40G node	9	4x10G/40G node

Cluster switch A		Cluster switch B	
10	4x10G/40G node	10	4x10G/40G node
11	4x10G/40G node	11	4x10G/40G node
12	4x10G/40G node	12	4x10G/40G node
13	4x10G/40G node	13	4x10G/40G node
14	4x10G/40G node	14	4x10G/40G node
15	4x10G/40G node	15	4x10G/40G node
16	4x10G/40G node	16	4x10G/40G node
17	4x10G/40G node	17	4x10G/40G node
18	4x10G/40G node	18	4x10G/40G node
19	40G node 19	19	40G node 19
20	40G node 20	20	40G node 20
21	40G node 21	21	40G node 21
22	40G node 22	22	40G node 22
23	40G node 23	23	40G node 23
24	40G node 24	24	40G node 24
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.

Cluster switch A		Cluster switch B	Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage	
1		1		
2		2		
3		3		
4		4		
5		5		
6		6		
7		7		
8		8		
9		9		
10		10		
11		11		
12		12		
13		13		
14		14		
15		15		
16		16		
17		17		
18		18		
19		19		
20		20		
21		21		

Cluster switch A		Cluster switch B	
22		22	
23		23	
24		24	
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Cisco Nexus 5596UP and 5596T cabling worksheet

If you want to document the supported platforms, you must complete the blank cabling worksheet by using the completed sample cabling worksheet as a guide.

Sample cabling worksheet

Some platforms support more than one 10GbE cluster port connection per cluster interconnect switch. To support additional cluster connections, you can use ports 25 through 40, as well as ports 49 through 80 when expansion modules are installed.

The sample port definition on each pair of switches is as follows:

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	Node port 1	1	Node port 1
2	Node port 2	2	Node port 2
3	Node port 3	3	Node port 3
4	Node port 4	4	Node port 4
5	Node port 5	5	Node port 5
6	Node port 6	6	Node port 6
7	Node port 7	7	Node port 7
8	Node port 8	8	Node port 8

Cluster switch A		Cluster switch B	
9	Node port 9	9	Node port 9
10	Node port 10	10	Node port 10
11	Node port 11	11	Node port 11
12	Node port 12	12	Node port 12
13	Node port 13	13	Node port 13
14	Node port 14	14	Node port 14
15	Node port 15	15	Node port 15
16	Node port 16	16	Node port 16
17	Node port 17	17	Node port 17
18	Node port 18	18	Node port 18
19	Node port 19	19	Node port 19
20	Node port 20	20	Node port 20
21	Node port 21	21	Node port 21
22	Node port 22	22	Node port 22
23	Node port 23	23	Node port 23
24	Node port 24	24	Node port 24
25 through 40	Reserved	25 through 40	Reserved
41	ISL to switch B port 41	41	ISL to switch A port 41
42	ISL to switch B port 42	42	ISL to switch A port 42
43	ISL to switch B port 43	43	ISL to switch A port 43
44	ISL to switch B port 44	44	ISL to switch A port 44
45	ISL to switch B port 45	45	ISL to switch A port 45

Cluster switch A		Cluster switch B	
46	ISL to switch B port 46	46	ISL to switch A port 46
47	ISL to switch B port 47	47	ISL to switch A port 47
48	ISL to switch B port 48	48	ISL to switch A port 48

Blank cabling worksheet

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster. The *Supported Cluster Connections* section of the *Hardware Universe* defines the cluster ports used by the platform.



Switch ports 1 through 24 function as 10 GbE ports. Switch ports 41 through 48 are reserved for Inter-Switch Links (ISLs).

Cluster switch A		Cluster switch B	
Switch port	Node/port usage	Switch port	Node/port usage
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	

Cluster switch A		Cluster switch B	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 40	Reserved	25 through 40	Reserved
41	ISL to switch B port 41	41	ISL to switch A port 41
42	ISL to switch B port 42	42	ISL to switch A port 42
43	ISL to switch B port 43	43	ISL to switch A port 43
44	ISL to switch B port 44	44	ISL to switch A port 44
45	ISL to switch B port 45	45	ISL to switch A port 45
46	ISL to switch B port 46	46	ISL to switch A port 46
47	ISL to switch B port 47	47	ISL to switch A port 47
48	ISL to switch B port 48	48	ISL to switch A port 48

Sample and blank cabling worksheets

The sample cabling worksheets provide examples of recommended port assignments

from the switches to the controllers. The blank worksheets provide a template that you can use in setting up your cluster.

Configure a new Cisco Nexus 92300YC switch

Configure a new Cisco Nexus 92300YC switch

You can configure a new Nexus 92300YC switch by completing the steps detailed in this chapter.

Installing the Nexus 92300YC switch on systems running ONTAP 9.6 and later, starts with setting up an IP address and configuration to allow the switch to communicate through the management interface. You can then install the NX-OS software and reference configuration file (RCF). This procedure is intended for preparing the Nexus 92300YC switch before controllers are added.

The examples in this procedure use the following switch and node nomenclature:

- The Nexus 92300YC switch names are cs1 and cs2.
- The example used in this procedure starts the upgrade on the second switch, *cs2*.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The IPspace name is Cluster.
- The cluster1::*> prompt indicates the name of the cluster.
- The cluster ports on each node are named e0a and e0b.

See the *Hardware Universe*[^] for the actual cluster ports supported on your platform.

- The Inter-Switch Links (ISLs) supported for the Nexus 92300YC switches are ports 1/65 and 1/66.
- The node connections supported for the Nexus 92300YC switches are ports 1/1 through 1/66.
- The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.

Initial installation of the Cisco Nexus 92300YC switch

You can use this procedure to perform the initial installation of the Cisco Nexus 92300YC switch.

About this task

You can download the applicable NetApp Cisco NX-OS software for your switches from the NetApp Support Site at mysupport.netapp.com

NX-OS is a network operating system for the Nexus series of Ethernet switches and MDS series of Fibre Channel (FC) storage area network switches provided by Cisco Systems.

This procedure provides a summary of the process to install your switches and get them running:

Steps

1. Connect the serial port to the host or serial port of your choice.

- Connect the management port (on the non-port side of the switch) to the same network where your SFTP server is located.
- 3. At the console, set the host side serial settings:
 - · 9600 baud
 - 8 data bits
 - 1 stop bit
 - parity: none
 - · flow control: none
- 4. Booting for the first time or rebooting after erasing the running configuration, the Nexus 92300YC switch loops in a boot cycle. Interrupt this cycle by typing **yes** to abort Power on Auto Provisioning. You are then presented with the System Admin Account setup:

```
$ VDC-1 %$ %POAP-2-POAP_INFO: - Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic configuration, no - continue with Power On Auto Provisioning] (yes/skip/no)[no]: *y*
Disabling POAP......Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please wait...
(This may take 5-15 minutes)

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

1. Type **y** to enforce secure password standard:

```
Do you want to enforce secure password standard (yes/no) [y]: {f y}
```

2. Enter and confirm the password for user admin:

```
Enter the password for "admin":
Confirm the password for "admin":
```

3. Enter the Basic System Configuration dialog:

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 Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 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.

Would you like to enter the basic configuration dialog (yes/no):

4. Create another login account:

```
Create another login account (yes/no) [n]:
```

5. Configure read-only and read-write SNMP community strings:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

6. Configure the cluster switch name:

```
Enter the switch name : cs2
```

7. Configure the out-of-band management interface:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address: 172.22.133.216

Mgmt0 IPv4 netmask: 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

8. Configure advanced IP options:

```
Configure advanced IP options? (yes/no) [n]: n
```

9. Configure Telnet services:

```
Enable the telnet service? (yes/no) [n]: n
```

10. Configure SSH services and SSH keys:

```
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]: 2048
```

11. Configure other settings:

```
Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L2]: L2

Configure default switchport interface state (shut/noshut) [noshut]: noshut

Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: strict
```

12. Confirm switch information and save the configuration:

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

Use this configuration and save it? (yes/no) [y]: y

[] 100%

Copy complete, now saving to disk (please wait)...

Copy complete.
```

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 92300YC switch.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the NX-OS software and EPLD images to the Nexus 92300YC switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.2.2.bin /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.2.2.img /bootflash/n9000-epld.9.2.2.img
/code/n9000-epld.9.2.2.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
```

4. Verify the running version of the NX-OS software:

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and unless otherwise stated, there is no warranty, express or implied, including
```

```
but not
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 05.31
 NXOS: version 9.2(1)
 BIOS compile time: 05/17/2018
 NXOS image file is: bootflash://nxos.9.2.1.bin
 NXOS compile time: 7/17/2018 16:00:00 [07/18/2018 00:21:19]
Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
 Processor Board ID FD0220329V5
 Device name: cs2
 bootflash: 115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)
Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
  System version: 9.2(1)
  Service:
plugin
 Core Plugin, Ethernet Plugin
Active Package(s):
cs2#
```

5. Install the NX-OS image.

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.2.2.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS
Verifying image type.
[] 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.2.2.bin.
[] 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
reset default upgrade is not
       yes disruptive
hitless
Images will be upgraded according to following table:
Module Image Running-Version(pri:alt
                                               New-Version
Upg-Required
_____
-----
 1 nxos
                                        9.2(1)
9.2(2)
           yes
 1 bios v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018) yes
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

2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully deactivated virtual service 'guestshell+'

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

6. Verify the new version of NX-OS software after the switch has rebooted:

show version

cs2# show version Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac Copyright (C) 2002-2018, Cisco and/or its affiliates. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and unless otherwise stated, there is no warranty, express or implied, including but not limited to warranties of merchantability and fitness for a particular purpose. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or GNU General Public License (GPL) version 3.0 or the GNU Lesser General Public License (LGPL) Version 2.1 or Lesser General Public License (LGPL) Version 2.0. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and

```
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
 BIOS: version 05.33
 NXOS: version 9.2(2)
 BIOS compile time: 09/08/2018
 NXOS image file is: bootflash:///nxos.9.2.2.bin
 NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FD0220329V5
 Device name: cs2
 bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)
Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
  Reason: Reset due to upgrade
  System version: 9.2(1)
  Service:
plugin
  Core Plugin, Ethernet Plugin
Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

EPLD Device		Version			
 MI FPGA		0x7			
IO FPGA		0x17			
MI FPGA2		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
cs2# instal :	epld bootfl	ash:n9000-epld.	9.2.2.img mod	dule 1	
Compatibilit	cy check:				
		Upgradable			
1		Yes			
	EPLD	Running	llowing table g-Version N		lon Upg-
Required 1 SUI	P MI FPGA	Running	9-Version N 	New-Versi 0x07 0x19	No Yes
Required 1 SUI 1 SUI 1 SUI 1 SUI The above mo	MI FPGA ONE OF TO FPGA ONE OF TO FPGA2 One of The Teles One of Teles One of Teles	e upgrade.	0x07 0x17 0x02	0x07 0x19 0x02	No Yes
Required 1 SUI 1 SUI 1 SUI The above mo	MI FPGA ONE OF TO FPGA ONE OF TO FPGA2 One of The Teles One of Teles One of Teles	e upgrade. ded at the end (y/n) ? $[n]$ y	0x07 0x17 0x02	0x07 0x19 0x02	 No Yes
Required 1 SUI 1 SUI 1 SUI The above monomorphic switch to the switch t	P MI FPGA P IO FPGA P MI FPGA2 Dodules require vill be reload	e upgrade. ded at the end of (y/n) ? $[n]$ \mathbf{y} dules.	0x07 0x17 0x02	0x07 0x19 0x02	No Yes
Required 1 SUI 1 SUI 1 SUI The above mo The switch w Do you want Proceeding to Starting Moo	P MI FPGA P IO FPGA P MI FPGA2 P	e upgrade. ded at the end ((y/n) ? [n] y dules. pgrade ramming] : 100.0	g-Version N 0x07 0x17 0x02 of the upgrad	New-Versi 0x07 0x19 0x02	No
Required 1 SUI 1 SUI 1 SUI 1 SUI The above mo The switch w Do you want Proceeding to Starting Moo Module 1: I Module 1 EPI Module	MI FPGA P IO FPGA P MI FPGA P MI FPGA2 P MI FPGA P M	e upgrade. ded at the end ((y/n) ? [n] y dules. pgrade ramming] : 100.0 successful. ade-Result	g-Version N 0x07 0x17 0x02 of the upgrac	New-Versi 0x07 0x19 0x02	No
Required 1 SUI 1 SUI 1 SUI 1 SUI The above mo The switch want Proceeding to Starting Mood Module 1: In Module 1 EPI Module	MI FPGA P IO FPGA P MI FPGA P MI FPGA2 P MI FPGA P M	e upgrade. ded at the end of (y/n) ? [n] y dules. pgrade ramming] : 100.0 successful. ade-Result	g-Version N 0x07 0x17 0x02 of the upgrac	New-Versi 0x07 0x19 0x02	No

8. After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

cs2# show version module	e 1 epld	
EPLD Device	Version	
MI FPGA	0x7	
IO FPGA	0x19	
MI FPGA2	0x2	
GEM FPGA	0x2	

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 92300YC switch for the first time.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the RCF to the Nexus 92300YC switch:

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt
/bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R 100% 9687 530.2KB/s 00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Merge the RCF with the running-config of the switch:

```
cs2# copy bootflash:Nexus 92300YC RCF v1.0.2.txt running-config
Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits).....
generated ecdsa key
Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
Edge port type (portfast) should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
Use with CAUTION
Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
have effect when the interface is in a non-trunking mode.
. . .
Copy complete, now saving to disk (please wait)...
Copy complete.
```

5. Verify on the switch that the RCF has been merged successfully:

show running-config

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019
version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
feature lacp
no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6 role network-admin
ssh key ecdsa 521
banner motd #
  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
  Ports 1/1 - 1/48: 10GbE Intra-Cluster Node Ports
  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
```

6. Save the running configuration so that it becomes the startup configuration when you reboot the switch:

```
cs2# *copy running-config startup-config*

[################################# 100%

Copy complete, now saving to disk (please wait)...

Copy complete.
```

7. For ONTAP 9.6P8 and later, enable the CSHM ASUP log collection feature for collecting switch-related log files: system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cs2# system cluster-switch log setup-password
Output example required here
cs2# system cluster-switch log enable-collection
Output example required here too
```

8. Reboot the switch and verify that the running configuration is correct:

reload

```
cs2# reload  
This command will reboot the system. (y/n)? [n] \mathbf{y}
```

Install NX-OS software and RCF on Cisco Nexus 92300YC cluster switches

Install NX-OS software and RCF on Cisco Nexus 92300YC cluster switches

The Cisco NX-OS software and reference configuration files (RCFs) must be installed on Cisco Nexus 92300YC cluster switches.

Before you begin

The following conditions must exist before you install the NX-OS software and Reference Configurations Files (RCFs) on the cluster switch:

- The cluster must be fully functioning (there should be no errors in the logs or similar issues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have consulted the switch compatibility table on the Cisco Ethernet switch page for the supported ONTAP, NX-OS, and RCF versions.
- There can be command dependencies between the command syntax in the RCF and that found in

versions of NX-OS.

- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on the Cisco Nexus 9000 Series Switches page.
- You must have the current RCF.

About this task

The examples in this procedure use two nodes. These nodes use two 10GbE cluster interconnect ports e0a and e0b.

See the Hardware Universe to verify the correct cluster ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

The examples in this procedure use the following switch and node nomenclature:

- The names of the two Cisco switches are cs1 and cs2.
- The node names are node1 and node2.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1 and node2_clus1 and node2_clus2 for node2.
- The cluster1::*> prompt indicates the name of the cluster.



The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.

Steps

1. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=x h
```

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster1:> system node autosupport invoke -node * -type all -message
MAINT=2h
```

3. Display how many cluster interconnect interfaces are configured in each node for each cluster interconnect switch: network device-discovery show -protocol cdp

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	 /cdp			
110402	e0a	cs1	Eth1/2	N9K-
C92300YC				
	e0b	cs2	Eth1/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C92300YC				
	e0b	cs2	Eth1/1	N9K-
C92300YC				

- 4. Check the administrative or operational status of each cluster interface.
 - a. Display the network port attributes:network port show -ipspace Cluster

cluster1:	:*> network p	ort show -i	ipspace	Clust	ter		
Node: nod	e2						
Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	
e0a	Cluster	Cluster		up	9000	auto/10000	healthy
e0b	Cluster	Cluster		up	9000	auto/10000	healthy
Node: nod	e1						
						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/10000	healthv
e0b	Cluster	Cluster		up	9000		_
4 entries	were display	ed.					

$b. \ \ \textbf{Display information about the LIFs:} \ \texttt{network interface show -} \textbf{vserver Cluster}$

cluster	1::*	> network in	nterface sho	ow -vserver Cluster	
		Logical	Status	Network	Current
Current	Is				
Vserver		Interface	Admin/Oper	Address/Mask	Node
Port	Hom	е			
		_			
Cluster					
		node1_clus1	l up/up	169.254.209.69/16	node1
e0a	tru				
		node1_clus2	2 up/up	169.254.49.125/16	node1
e0b	tru				
		node2_clus1	l up/up	169.254.47.194/16	node2
e0a	tru				
		node2_clus2	2 up/up	169.254.19.183/16	node2
e0b	tru	е			
4 entri	es w	ere displaye	ed.		

5. Ping the remote cluster LIFs:

cluster ping-cluster -node node-name

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
Cluster node1 clus2 169.254.49.125 node1
                                             e0b
Cluster node2 clus1 169.254.47.194 node2
                                             e0a
Cluster node2 clus2 169.254.19.183 node2
                                             e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Verify that the auto-revert command is enabled on all cluster LIFs:

network interface show -vserver Cluster -fields auto-revert

7. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files using the commands:

system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y|n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 92300YC switch.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the NX-OS software and EPLD images to the Nexus 92300YC switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.2.2.bin /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1
Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.2.2.img /bootflash/n9000-epld.9.2.2.img
/code/n9000-epld.9.2.2.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait) ...
Copy complete.
```

4. Verify the running version of the NX-OS software:

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 05.31
 NXOS: version 9.2(1)
 BIOS compile time: 05/17/2018
 NXOS image file is: bootflash://nxos.9.2.1.bin
 NXOS compile time: 7/17/2018 16:00:00 [07/18/2018 00:21:19]
Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FD0220329V5
  Device name: cs2
  bootflash: 115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)
Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
  System version: 9.2(1)
```

```
Service:

plugin
Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. Install the NX-OS image.

Installing the image file causes it to be loaded every time the switch is rebooted.

```
cs2# install all nxos bootflash:nxos.9.2.2.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS
Verifying image type.
[] 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos.9.2.2.bin.
[] 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
                                             9.2(1)
9.2(2)
            yes
 1 bios v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018) yes
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
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION STATE:
Successfully deactivated virtual service 'guestshell+'
Finishing the upgrade, switch will reboot in 10 seconds.
```

6. Verify the new version of NX-OS software after the switch has rebooted:

show version

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
```

```
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
 BIOS: version 05.33
 NXOS: version 9.2(2)
 BIOS compile time: 09/08/2018
 NXOS image file is: bootflash://nxos.9.2.2.bin
 NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
 Processor Board ID FD0220329V5
  Device name: cs2
 bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)
Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
  Reason: Reset due to upgrade
  System version: 9.2(1)
  Service:
plugin
 Core Plugin, Ethernet Plugin
Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

EPLD Device		Version			
 MI FPGA		0x7			
IO FPGA		0x17			
MI FPGA2		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
GEM FPGA		0x2			
cs2# install	epld bootfla	ash:n9000-epld.	9.2.2.img	module 1	
Compatibility	y check:				
		Upgradable	_		ı
 1		 Yes			
1	201	162	arsrupt	live Module	: Opgradable
Module Type		according to folk	_		on Upg-
_		_	_		on Upg-
Module Type Required		_	g-Version		
Module Type Required 1 SUP	EPLD	_	0x07 0x17	New-Versi 0x07 0x19	 No
Module Type Required 1 SUP 1 SUP 1 SUP	EPLD MI FPGA IO FPGA MI FPGA2	Running	g-Version 0x07	New-Versi 0x07 0x19	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP 1 SUP	EPLD MI FPGA IO FPGA MI FPGA2 dules require	Running	0x07 0x17 0x02	New-Versi 0x07 0x19 0x02	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP The above module The switch with support	EPLD MI FPGA IO FPGA MI FPGA2 dules require	Running e upgrade. ded at the end o	0x07 0x17 0x02	New-Versi 0x07 0x19 0x02	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP The above module	EPLD MI FPGA IO FPGA MI FPGA2 dules require	Running	0x07 0x17 0x02	New-Versi 0x07 0x19 0x02	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch will Do you want	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue	Running e upgrade. ded at the end ((y/n) ? [n] y	0x07 0x17 0x02	New-Versi 0x07 0x19 0x02	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP The above module	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue	Running e upgrade. ded at the end ((y/n) ? [n] y	0x07 0x17 0x02	New-Versi 0x07 0x19 0x02	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch will Do you want	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue o upgrade Mod	Running e upgrade. ded at the end of (y/n) ? [n] y dules.	0x07 0x17 0x02	New-Versi 0x07 0x19 0x02	 No Yes
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch witch witch witch Do you want to	EPLD MI FPGA IO FPGA MI FPGA2 dules required in the reload to continue to upgrade Modules	Running e upgrade. ded at the end of (y/n) ? [n] y dules. pgrade	g-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch witch witch Do you want to Proceeding to Starting Module Module 1: Id	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue upgrade Mod ale 1 EPLD Up	Running e upgrade. ded at the end of (y/n) ? [n] y dules. pgrade ramming] : 100.0	g-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch witch witch witch Proceeding to Starting Modu Module 1: Id Module 1 EPLI	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue upgrade Mod ale 1 EPLD Up FPGA [Prog:	Running e upgrade. ded at the end (y/n) ? [n] y dules. pgrade ramming] : 100.0 successful.	g-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch with Do you want to Proceeding to Starting Module Module 1: Id Module 1 EPLI	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue upgrade Mod ale 1 EPLD Up FPGA [Prog: Upgrade is Type Upgra	Running e upgrade. ded at the end (y/n) ? [n] y dules. pgrade ramming] : 100.0 successful.	9-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No
Module Type Required 1 SUP 1 SUP 1 SUP The above mod The switch witch witch witch Proceeding to Starting Module Module 1 : Id Module 1 EPLI Module	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue upgrade Mod ale 1 EPLD Up FPGA [Prog: Upgrade is Type Upgrade	Running e upgrade. ded at the end of (y/n) ? [n] y dules. pgrade ramming] : 100.0 successful. ade-Result	9-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No
Module Type Required 1 SUP 1 SUP 1 SUP 1 SUP The above mod The switch witch w	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue upgrade Mod ale 1 EPLD Up FPGA [Prog: Upgrade is Type Upgra	Running e upgrade. ded at the end of (y/n) ? [n] y dules. pgrade ramming] : 100.0 successful. ade-Result	9-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No
Module Type Required 1 SUP 1 SUP 1 SUP 1 SUP The above mod The switch witch w	EPLD MI FPGA IO FPGA MI FPGA2 dules require ill be reload to continue upgrade Mod ale 1 EPLD Up FPGA [Prog: Upgrade is Type Upgrade	Running e upgrade. ded at the end of (y/n) ? [n] y dules. pgrade ramming] : 100.0 successful. ade-Result	9-Version 0x07 0x17 0x02 of the upo	New-Versi 0x07 0x19 0x02 grade	 No Yes No

8. After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

cs2# show version module 1 epld	
EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x19
MI FPGA2	0x2
GEM FPGA	0x2

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 92300YC switch for the first time.

Steps

- 1. Connect the cluster switch to the management network.
- 2. Use the ping command to verify connectivity to the server hosting the RCF.

This example verifies that the switch can reach the server at IP address 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copy the RCF to the Nexus 92300YC switch:

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt
/bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R 100% 9687 530.2KB/s 00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Merge the RCF with the running-config of the switch:

```
cs2# copy bootflash:Nexus 92300YC RCF v1.0.2.txt running-config
Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits).....
generated ecdsa key
Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
Edge port type (portfast) should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
Use with CAUTION
Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
have effect when the interface is in a non-trunking mode.
. . .
Copy complete, now saving to disk (please wait)...
Copy complete.
```

5. Verify on the switch that the RCF has been merged successfully:

show running-config

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019
version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
feature lacp
no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6 role network-admin
ssh key ecdsa 521
banner motd #
  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
  Ports 1/1 - 1/48: 10GbE Intra-Cluster Node Ports
  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
```

6. Save the running configuration so that it becomes the startup configuration when you reboot the switch:

```
cs2# copy running-config startup-config

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. For ONTAP 9.6P8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```

8. Reboot the switch and verify that the running configuration is correct:

reload

```
cs2# reload  
This command will reboot the system. (y/n)? [n] {\bf y}
```

Migrate to a two-node switched cluster with Cisco Nexus 92300YC switches

Migrate to a two-node switched cluster with Cisco Nexus 92300YC switches

You must be aware of certain configuration information, port connections, and cabling requirements when you migrate a two-node switchless cluster, non-disruptively, to a cluster with Cisco Nexus 92300YC cluster switches. The procedure you use depends on whether you have two dedicated cluster-network ports on each controller or a single cluster port on each controller. The process documented works for all nodes using optical or twinax ports but is not supported on this switch if nodes are using onboard 10Gb BASE-T RJ45 ports for the cluster-network ports.

Most systems require two dedicated cluster-network ports on each controller.



After your migration completes, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for 92300YC cluster switches. See *Installing the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches* in the Setting up guide.

How to migrate to a two-node switched cluster with a Cisco Nexus 92300YC switch

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using Cisco Nexus 92300YC switches to enable you to scale beyond two nodes in the cluster.

Before you begin

Two-node switchless configuration:

- The two-node switchless configuration must be properly set up and functioning.
- The nodes must be running ONTAP 9.6 and later.
- All cluster ports must be in the up state.
- All cluster logical interfaces (LIFs) must be in the up state and on their home ports.

Cisco Nexus 92300YC switch configuration:

· Both switches must have management network connectivity.

- There must be console access to the cluster switches.
- Nexus 92300YC node-to-node switch and switch-to-switch connections must use twinax or fiber cables.

The Hardware Universe - Switches contains more information about cabling.

- Inter-Switch Link (ISL) cables must be connected to ports 1/65 and 1/66 on both 92300YC switches.
- Initial customization of both the 92300YC switches must be completed. So that the:
 - 92300YC switches are running the latest version of software
 - Reference Configuration Files (RCFs) have been applied to the switches
 Any site customization, such as SMTP, SNMP, and SSH must be configured on the new switches.

About this task

The examples in this procedure use the following cluster switch and node nomenclature:

- The names of the 92300YC switches are cs1 and cs2.
- The names of the cluster SVMs are node1 and node2.
- The names of the LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- The cluster1::*> prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e0a and e0b.

The *Hardware Universe* contains the latest information about the actual cluster ports for your platforms.

Steps

1. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

2. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster1::*> system node autosupport invoke -node * -type all -message
MAINT=2h
```

3. Disable all node-facing ports (not ISL ports) on both the new cluster switches cs1 and cs2.

You must not disable the ISL ports.

The following example shows that node-facing ports 1 through 64 are disabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e/1-64
cs1(config-if-range)# shutdown
```

4. Verify that the ISL and the physical ports on the ISL between the two 92300YC switches cs1 and cs2 are up on ports 1/65 and 1/66:

```
show port-channel summary
```

The following example shows that the ISL ports are up on switch cs1:

```
Csl# show port-channel summary

Flags: D - Down P - Up in port-channel (members)
    I - Individual H - Hot-standby (LACP only)
    s - Suspended r - Module-removed
    b - BFD Session Wait
    S - Switched R - Routed
    U - Up (port-channel)
    p - Up in delay-lacp mode (member)
    M - Not in use. Min-links not met

------

Group Port- Type Protocol Member Ports
    Channel
-------
1 Pol(SU) Eth LACP Eth1/65(P) Eth1/66(P)
```

The following example shows that the ISL ports are up on switch cs2:

5. Display the list of neighboring devices:

```
show cdp neighbors
```

This command provides information about the devices that are connected to the system.

The following example lists the neighboring devices on switch cs1:

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute

Device-ID Local Intrfce Hldtme Capability Platform Port ID cs2(FD0220329V5) Eth1/65 175 R S I s N9K-C92300YC Eth1/65 cs2(FD0220329V5) Eth1/66 175 R S I s N9K-C92300YC Eth1/66

Total entries displayed: 2
```

The following example lists the neighboring devices on switch cs2:

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Port ID cs1(FD0220329KU) Eth1/65 177 R S I s N9K-C92300YC Eth1/65 cs1(FD0220329KU) Eth1/66 177 R S I s N9K-C92300YC Eth1/66 Total entries displayed: 2

6. Verify that all cluster ports are up:

network port show -ipspace Cluster

Each port should display up for Link and healthy for Health Status.

cluster1::*> network port show -ipspace Cluster Node: node1 Speed (Mbps) Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status Cluster up 9000 auto/10000 healthy Cluster up 9000 auto/10000 healthy e0a Cluster e0b Cluster Node: node2 Speed (Mbps) Health Port IPspace Broadcast Domain Link MTU Admin/Oper Status e0a Cluster Cluster up 9000 auto/10000 healthy e0b Cluster Cluster up 9000 auto/10000 healthy 4 entries were displayed.

7. Verify that all cluster LIFs are up and operational:

network interface show -vserver Cluster

<pre>cluster1::*> network interface show -vserver Cluster</pre>								
	Logical	Status	Network	Current				
Current Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
Cluster								
	node1_clus1	l up/up	169.254.209.69/16	node1	e0a			
true								
	node1_clus2	2 up/up	169.254.49.125/16	node1	e0b			
true								
	node2_clus1	l up/up	169.254.47.194/16	node2	e0a			
true			160 054 10 100 /55	1 0	0.1			
	node2_clus2	2 up/up	169.254.19.183/16	node2	e0b			
true	1.	,						
4 entries we	ere displaye	ea.						

8. Verify that auto-revert is enabled on all cluster LIFs:

network interface show -vserver Cluster -fields auto-revert

9. Disconnect the cable from cluster port e0a on node1, and then connect e0a to port 1 on cluster switch cs1, using the appropriate cabling supported by the 92300YC switches.

The Hardware Universe - Switches contains more information about cabling.

10. Disconnect the cable from cluster port e0a on node2, and then connect e0a to port 2 on cluster switch cs1, using the appropriate cabling supported by the 92300YC switches.

11. Enable all node-facing ports on cluster switch cs1.

The following example shows that ports 1/1 through 1/64 are enabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

12. Verify that all cluster LIFs are up, operational, and display as true for Is Home:

network interface show -vserver Cluster

The following example shows that all of the LIFs are up on node1 and node2 and that Is Home results are true:

	Logical	Status	Network	Current	Current
Is	-				
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
true	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true	node2_clus2	up/up	169.254.19.183/16	node2	e0b

13. Display information about the status of the nodes in the cluster:

cluster show

The following example displays information about the health and eligibility of the nodes in the cluster:

```
Node Health Eligibility Epsilon
-----
node1 true true false
node2 true true false

2 entries were displayed.
```

- 14. Disconnect the cable from cluster port e0b on node1, and then connect e0b to port 1 on cluster switch cs2, using the appropriate cabling supported by the 92300YC switches.
- 15. Disconnect the cable from cluster port e0b on node2, and then connect e0b to port 2 on cluster switch cs2, using the appropriate cabling supported by the 92300YC switches.
- 16. Enable all node-facing ports on cluster switch cs2.

The following example shows that ports 1/1 through 1/64 are enabled on switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-64
cs2(config-if-range)# no shutdown
```

17. Verify that all cluster ports are up:

```
network port show -ipspace Cluster
```

The following example shows that all of the cluster ports are up on node1 and node2:

<pre>cluster1::*> network port show -ipspace Cluster</pre>								
Node: nod	e1							
Ignore						Cura and (Mlassa)	II.a.a.l.t.b	
Health						Speed (Mbps)	неатсп	
	IPspace					_		
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy	
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy	
Node: nod	e2							
Ignore						Speed(Mbps)	Health	
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy	
	Cluster	Cluster		up	9000	auto/10000	healthy	
4 entries were displayed.								

18. Verify that all interfaces display true for ${\tt Is}\ {\tt Home}$:

network interface show -vserver Cluster



This might take several minutes to complete.

The following example shows that all LIFs are up on node1 and node2 and that Is Home results are true:

cluster1::*> network interface show -vserver Cluster								
	Logical	Status	Network	Current	Current			
Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
Cluster								
	node1_clus1	up/up	169.254.209.69/16	node1	e0a			
true								
	node1_clus2	up/up	169.254.49.125/16	node1	e0b			
true								
	node2_clus1	up/up	169.254.47.194/16	node2	e0a			
true		,						
	node2_clus2	up/up	169.254.19.183/16	node2	e0b			
true								
4 entries were displayed.								

19. Verify that both nodes each have one connection to each switch:

show cdp neighbors

The following example shows the appropriate results for both switches:

(cs1) # show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID	Local Intrfce	Hldtme Capability	Platform	Port
ID				
node1	Eth1/1	133 Н	FAS2980	e0a
node2	Eth1/2	133 Н	FAS2980	e0a
cs2(FD0220329V5)	Eth1/65	175 RSIs	N9K-C92300YC	
Eth1/65				
cs2(FD0220329V5)	Eth1/66	175 RSIs	N9K-C92300YC	
Eth1/66				

Total entries displayed: 4

(cs2) # show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port
ID					
node1	Eth1/1	133	Н	FAS2980	e0b
node2	Eth1/2	133	Н	FAS2980	e0b
cs1(FD0220329KU)					
	Eth1/65	175	R S I s	N9K-C92300YC	
Eth1/65					
cs1(FD0220329KU)					
	Eth1/66	175	RSIs	N9K-C92300YC	
Eth1/66					

Total entries displayed: 4

20. Display information about the discovered network devices in your cluster:

network device-discovery show -protocol cdp

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	0/2	N9K-
C92300YC				
	e0b	cs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C92300YC				
	e0b	cs2	0/1	N9K-
C92300YC				

21. Verify that the settings are disabled:

network options switchless-cluster show



It might take several minutes for the command to complete. Wait for the '3 minute lifetime to expire' announcement.

The false output in the following example shows that the configuration settings are disabled:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

22. Verify the status of the node members in the cluster:

cluster show

The following example shows information about the health and eligibility of the nodes in the cluster:

```
Node Health Eligibility Epsilon

nodel true true false

node2 true true false
```

23. Ensure that the cluster network has full connectivity:

```
cluster1::> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e0a
Cluster node1 clus2 169.254.49.125 node1 e0b
Cluster node2 clus1 169.254.47.194 node2 e0a
Cluster node2 clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

24. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

```
cluster1::*> system node autosupport invoke -node * -type all -message
MAINT=END
```

25. Change the privilege level back to admin:

```
set -privilege admin
```

26. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

```
\verb|system| cluster-switch| log| setup-password| \verb|and| system| cluster-switch| log| enable-collection|
```

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y | n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Migrate from a Cisco switch to a Cisco Nexus 92300YC switch

Migrate from a Cisco switch to a Cisco Nexus 92300YC switch

You must be aware of certain configuration information, port connections and cabling requirements when you are replacing some older Cisco Nexus cluster switches with

Cisco Nexus 92300YC cluster switches.

- The following cluster switches are supported:
 - Nexus 92300YC
 - Nexus 5596UP
 - Nexus 5020
 - Nexus 5010
- The cluster switches use the following ports for connections to nodes:
 - Ports e1/1-48 (10/25 GbE), e1/49-64 (40/100 GbE): Nexus 92300YC
 - Ports e1/1-40 (10 GbE): Nexus 5596UP
 - Ports e1/1-32 (10 GbE): Nexus 5020
 - ∘ Ports e1/1-12, e2/1-6 (10 GbE): Nexus 5010 with expansion module
- The cluster switches use the following Inter-Switch Link (ISL) ports:
 - Ports e1/65-66 (100 GbE): Nexus 92300YC
 - Ports e1/41-48 (10 GbE): Nexus 5596UP
 - Ports e1/33-40 (10 GbE): Nexus 5020
 - Ports e1/13-20 (10 GbE): Nexus 5010
- The Hardware Universe Switches contains information about supported cabling for all cluster switches.
- You have configured some of the ports on Nexus 92300YC switches to run at 10 GbE or 40 GbE.
- You have planned, migrated, and documented 10 GbE and 40 GbE connectivity from nodes to Nexus 92300YC cluster switches.
- The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page.



After your migration completes, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for 92300YC cluster switches. See *Installing the Cluster Switch Health Monitor (CSHM) configuration file for 92300YC switches* in the Setting up guide.

How to migrate from a Cisco switch to a Cisco Nexus 92300YC switch

You can migrate nondisruptively older Cisco cluster switches for an ONTAP cluster to Cisco Nexus 92300YC cluster network switches.

About this task

- The existing cluster must be properly set up and functioning.
- All cluster ports must be in the up state to ensure nondisruptive operations.
- The Nexus 92300YC cluster switches must be configured and operating under the proper version of NX-OS installed and reference configuration file (RCF) applied.
- The existing cluster network configuration must have the following:
 - A redundant and fully functional NetApp cluster using both older Cisco switches.
 - Management connectivity and console access to both the older Cisco switches and the new switches.

- All cluster LIFs in the up state with the cluster LIFs are on their home ports.
- ISL ports enabled and cabled between the older Cisco switches and between the new switches.

The examples in this procedure use the following switch and node nomenclature:

- The existing Cisco Nexus 5596UP cluster switches are c1 and c2.
- The new Nexus 92300YC cluster switches are cs1 and cs2.
- The nodes are node1 and node2.
- The cluster LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- Switch c2 is replaced by switch cs2 first and then switch c1 is replaced by switch cs1.
 - A temporary ISL is built on cs1 connecting c1 to cs1.
 - Cabling between the nodes and c2 are then disconnected from c2 and reconnected to cs2.
 - Cabling between the nodes and c1 are then disconnected from c1 and reconnected to cs1.
 - The temporary ISL between c1 and cs1 is then removed.

Steps

1. Change the privilege level to advanced, entering **y** when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

2. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster1::*> system node autosupport invoke -node * -type all -message
MAINT=2h
```

3. Verify that auto-revert is enabled on all cluster LIFs:

network interface show -vserver Cluster -fields auto-revert

```
Cluster1::*> network interface show -vserver Cluster -fields auto-revert

Logical
Vserver Interface Auto-revert

Cluster

node1_clus1 true
node1_clus2 true
node2_clus1 true
node2_clus1 true
node2_clus2 true

4 entries were displayed.
```

4. Determine the administrative or operational status for each cluster interface:

Each port should display up for Link and healthy for Health Status.

a. Display the network port attributes:

network port show -ipspace Cluster

cluster1:	:*> network p	ort show -	ipspace	Clus	ter			
Node: nod	e1							
Ignore						0 1/25		
Health						Speed (Mbps)	Health	
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy	
	Cluster	Cluster		up	9000	auto/10000	healthy	
false								
Node: nod	e2							
Ignore								
71						Speed(Mbps)	Health	
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy	
	Cluster	Cluster		up	9000	auto/10000	healthy	
4 entries	4 entries were displayed.							

b. Display information about the logical interfaces and their designated home nodes:

network interface show -vserver Cluster

Each LIF should display up/up for Status Admin/Oper and true for Is Home.

cluster1::*> network interface show -vserver Cluster								
		Logical	Status	Network	Current			
Current	Is							
Vserver		Interface	Admin/Oper	Address/Mask	Node			
Port	Home							
Cluster								
		node1_clus1	up/up	169.254.209.69/16	node1			
e0a	true	2						
		node1_clus2	up/up	169.254.49.125/16	node1			
e0b	true	2						
		node2_clus1	up/up	169.254.47.194/16	node2			
e0a	true							
		node2_clus2	up/up	169.254.19.183/16	node2			
e0b	true							
4 entrie	es we	ere displayed.						

5. The cluster ports on each node are connected to existing cluster switches in the following way (from the nodes' perspective) using the command:

network device-discovery show -protocol cdp

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID) Interface	Platform
node2	/cdp			
	e0a	c1	0/2	N5K-
C5596UP				
	e0b	c2	0/2	N5K-
C5596UP				
node1	/cdp			
	e0a	c1	0/1	N5K-
C5596UP				
	e0b	c2	0/1	N5K-
C5596UP				

6. The cluster ports and switches are connected in the following way (from the switches' perspective) using the command:

c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID Port ID	Local Intrf	ce Hldtn	ne Capabil:	ity Platform
node1	Eth1/1	124	Н	FAS2750
node2 e0a	Eth1/2	124	Н	FAS2750
c2(FOX2025GEFC) Eth1/41	Eth1/41	179	SIS	N5K-C5596UP
c2(FOX2025GEFC) Eth1/42	Eth1/42	175	SIS	N5K-C5596UP
c2(FOX2025GEFC) Eth1/43	Eth1/43	179	SIS	N5K-C5596UP
c2(FOX2025GEFC) Eth1/44	Eth1/44	175	SIS	N5K-C5596UP
c2(FOX2025GEFC) Eth1/45	Eth1/45	179	SIS	N5K-C5596UP
c2(FOX2025GEFC) Eth1/46	Eth1/46	179	SIS	N5K-C5596UP
c2(FOX2025GEFC) Eth1/47	Eth1/47	175	SIs	N5K-C5596UP
c2(FOX2025GEFC) Eth1/48	Eth1/48	179	SIs	N5K-C5596UP

Total entries displayed: 10

c2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

	S - Switch, H V - VoIP-Phon s - Supports-	e, D - Ren	motely-Ma	r - Repeater, naged-Device,	
Device-ID Port ID	Local Int	rfce Hldtr	me Capabi	lity Platform	
node1 e0b	Eth1/1	124	Н	FAS2750	
node2 e0b	Eth1/2	124	Н	FAS2750	
	Eth1/41	175	SIs	N5K-C5596UP	
c1(FOX2025GEEX) Eth1/42	Eth1/42	175	SIs	N5K-C5596UP	
c1(FOX2025GEEX) Eth1/43	Eth1/43	175	SIs	N5K-C5596UP	
c1(FOX2025GEEX) Eth1/44	Eth1/44	175	SIs	N5K-C5596UP	
c1(FOX2025GEEX) Eth1/45	Eth1/45	175	SIs	N5K-C5596UP	
c1(FOX2025GEEX) Eth1/46	Eth1/46	175	SIs	N5K-C5596UP	
c1(FOX2025GEEX) Eth1/47	Eth1/47	176	SIs	N5K-C5596UP	
c1 (FOX2025GEEX)	Eth1/48	176	SIs	N5K-C5596UP	

7. Ensure that the cluster network has full connectivity using the command:

cluster ping-cluster -node node-name

Eth1/48

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
Cluster node1 clus2 169.254.49.125 node1
                                               e0b
Cluster node2 clus1 169.254.47.194 node2
                                               e0a
Cluster node2 clus2 169.254.19.183 node2
                                               e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

8. Configure a temporary ISL on cs1on ports e1/41-48, between c1 and cs1.

The following example shows how the new ISL is configured on c1 and cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config) # interface e1/41-48
cs1(config-if-range)# description temporary ISL between Nexus 5596UP and
Nexus 92300YC
cs1(config-if-range)# no lldp transmit
cs1(config-if-range)# no lldp receive
cs1(config-if-range)# switchport mode trunk
cs1(config-if-range) # no spanning-tree bpduguard enable
cs1(config-if-range)# channel-group 101 mode active
cs1(config-if-range)# exit
cs1(config) # interface port-channel 101
cs1(config-if) # switchport mode trunk
cs1(config-if)# spanning-tree port type network
cs1(config-if)# exit
cs1(config)# exit
```

- 9. Remove ISL cables from ports e1/41-48 from c2 and connect the cables to ports e1/41-48 on cs1.
- 10. Verify that the ISL ports and port-channel are operational connecting c1 and cs1:

```
show port-channel summary
```

The following example shows the Cisco show port-channel summary command being used to verify the ISL ports are operational on c1 and cs1:

```
c1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/41(P) Eth1/42(P)
Eth1/43(P)
                                Eth1/44(P) Eth1/45(P)
Eth1/46(P)
                                 Eth1/47(P) Eth1/48(P)
cs1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/65(P) Eth1/66(P)
101 Po101(SU) Eth LACP
                                Eth1/41(P) Eth1/42(P)
Eth1/43(P)
                                Eth1/44(P) Eth1/45(P)
Eth1/46(P)
                                 Eth1/47(P) Eth1/48(P)
```

11. For node1, disconnect the cable from e1/1 on c2, and then connect the cable to e1/1 on cs2, using

- appropriate cabling supported by Nexus 92300YC.
- 12. For node2, disconnect the cable from e1/2 on c2, and then connect the cable to e1/2 on cs2, using appropriate cabling supported by Nexus 92300YC.
- 13. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

network device-discovery show -protocol cdp

		Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	c1	0/2	N5K-
C5596UP				
	e0b	cs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	c1	0/1	N5K-
C5596UP				
	e0b	cs2	0/1	N9K-
C92300YC				

- 14. For node1, disconnect the cable from e1/1 on c1, and then connect the cable to e1/1 on cs1, using appropriate cabling supported by Nexus 92300YC.
- 15. For node2, disconnect the cable from e1/2 on c1, and then connect the cable to e1/2 on cs1, using appropriate cabling supported by Nexus 92300YC.
- 16. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

network device-discovery show -protocol cdp

```
cluster1::*> network device-discovery show -protocol cdp
Node/ Local Discovered
         Port Device (LLDP: ChassisID) Interface
                                                       Platform
Protocol
node2 /cdp
                                        0/2
         e0a cs1
                                                       N9K-
C92300YC
         e0b cs2
                                        0/2
                                                       N9K-
C92300YC
node1 /cdp
         e0a
               cs1
                                        0/1
                                                       N9K-
C92300YC
         e0b cs2
                                        0/1
                                                       N9K-
C92300YC
4 entries were displayed.
```

17. Delete the temporary ISL between cs1 and c1.

```
cs1(config)# no interface port-channel 10
cs1(config)# interface e1/41-48
cs1(config-if-range)# lldp transmit
cs1(config-if-range)# lldp receive
cs1(config-if-range)# no switchport mode trunk
cs1(config-if-range)# no channel-group
cs1(config-if-range)# description 10GbE Node Port
cs1(config-if-range)# spanning-tree bpduguard enable
cs1(config-if-range)# exit
cs1(config)# exit
```

18. Verify the final configuration of the cluster:

```
network port show -ipspace Cluster
```

Each port should display up for Link and healthy for Health Status.

```
Cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore

Speed(Mbps) Health

Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
```

Status							
	Cluster	Cluster		up	9000	auto/10000	healthy
false		e-7			0000	. /1.0000	
	Cluster	Cluster		up	9000	auto/10000	healthy
false							
Node: node2	2						
Ignore							
						Speed (Mbps)	Health
Health -						1 /-	
	[Pspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status 							
e0a C	Cluster	Cluster		up	9000	auto/10000	healthy
false							_
e0b C	Cluster	Cluster		up	9000	auto/10000	healthy
false							
4 entries w	vere displaye						
4 entries w	were displaye *> network in Logical	nterface sh			Clust	cer Current	
4 entries w	> network i	nterface sh			Clust		
4 entries w	> network i	nterface sh	Netwo	rk			Port
4 entries w cluster1::* Current Is Vserver	> network i	nterface sh Status	Netwo	rk		Current	Port
4 entries w cluster1::* Current Is Vserver Home	> network i	nterface sh Status	Netwo	rk		Current	Por†
4 entries w cluster1::* Current Is Vserver Home	> network i	nterface sh Status Admin/Oper	Networ	rk ss/Mas	5k 	Current Node	Port e0a
4 entries w cluster1::* Current Is Vserver Home Cluster	Logical Interface	nterface sh Status Admin/Oper	Networ	rk ss/Mas	5k 	Current Node	
4 entries w cluster1::* Current Is Vserver Home Cluster	Logical Interface	Status Admin/Oper	Network Addres	rk ss/Mas	sk 9.69/1	Current Node	
4 entries w cluster1::* Current Is Vserver Home Cluster true	Logical Interface node1_clus	Status Admin/Oper	Network Addres	rk ss/Mas	sk 9.69/1	Current Node	 e0a
4 entries w cluster1::* Current Is Vserver Home Cluster true	Logical Interface node1_clus	Status Admin/Oper	Network Address 169.25	rk ss/Mas 54.209	sk 9.69/1	Current Node node node1 node1	 e0a
4 entries w cluster1::* Current Is Vserver	Logical Interface node1_clus: node2_clus:	Status Admin/Oper 1 up/up 2 up/up 1 up/up	Network Address 169.25 169.25	rk ss/Mas 54.209 54.49	sk 9.69/1 .125/1	Current Node node1 node1 node2	e0a e0b e0a
4 entries w cluster1::* Current Is Vserver Home Cluster true true	Logical Interface node1_clus2	Status Admin/Oper 1 up/up 2 up/up 1 up/up	Network Address 169.25 169.25	rk ss/Mas 54.209 54.49	sk 9.69/1 .125/1	Current Node node1 node1 node2	e0a e0b
4 entries w cluster1::* Current Is Vserver Home Cluster true true	Logical Interface node1_clus: node2_clus:	Status Admin/Oper 1 up/up 2 up/up 1 up/up	Network Address 169.25 169.25	rk ss/Mas 54.209 54.49	sk 9.69/1 .125/1	Current Node node1 node1 node2	e0a e0b e0a
4 entries was cluster1::* Current Is Vserver Home Cluster true true true	Logical Interface node1_clus: node1_clus: node2_clus: node2_clus:	Status Admin/Oper 1 up/up 2 up/up 1 up/up 2 up/up 2 up/up	Network Address 169.25 169.25	rk ss/Mas 54.209 54.49	sk 9.69/1 .125/1	Current Node node1 node1 node2	e0a e0b e0a
d entries we cluster1::* Current Is Vserver Home Cluster true true true	Logical Interface node1_clus: node2_clus:	Status Admin/Oper 1 up/up 2 up/up 1 up/up 2 up/up 2 up/up	Network Address 169.25 169.25	rk ss/Mas 54.209 54.49	sk 9.69/1 .125/1	Current Node node1 node1 node2	e0a e0b e0a

Device (LLDP: cs1 cs2	ChassisID)	0/2 0/2	ace 	Platform
cs2				N9K-
		0/2		
		0/2		
				N9K-
4				
		0 /1		
cs1		0/1		N9K-
002		0 / 1		NOV
CSZ		U/I		N9K-
ртауса.				
hbors				
S - Switch, H - V - VoIP-Phone,	Host, I - D - Remote	IGMP, r	- Repeater,	_
5 Suppores Si	1 Dispute			
Local Intrfce	Hldtme Cap	ability	Platform	Port
Eth1/1	124 Н		FAS2750	
Eth1/2	124 н		FAS2750	
	170 D	STG	N9K-C92300Y	7.0
Eth1/65	179 R	5 1 5	1,311 0,2000	
	S - Switch, H - V - VoIP-Phone, s - Supports-ST Local Intrfce Eth1/1	played. hbors R - Router, T - Trans-Brid S - Switch, H - Host, I - V - VoIP-Phone, D - Remote s - Supports-STP-Dispute Local Intrfce Hldtme Cap Eth1/1 124 H	played. hbors R - Router, T - Trans-Bridge, B - S - Switch, H - Host, I - IGMP, r V - VoIP-Phone, D - Remotely-Manages - Supports-STP-Dispute Local Intrfce Hldtme Capability Eth1/1 124 H	played. hbors R - Router, T - Trans-Bridge, B - Source-Rout S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Local Intrfce Hldtme Capability Platform Eth1/1 124 H FAS2750

ID node1	Eth1/1	124	Н	FAS2750
e0b node2 e0b	Eth1/2	124	Н	FAS2750
cs1(FDO220329KU) Eth1/65	Eth1/65	179	R S I s	N9K-C92300YC
cs1(FDO220329KU) Eth1/66	Eth1/66	179	RSIs	N9K-C92300YC

Total entries displayed: 4

19. Ensure that the cluster network has full connectivity:

cluster ping-cluster -node node-name

```
cluster1::*> set -priv advanced
Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? \{y|n\}: y
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1
Cluster node1 clus2 169.254.49.125 node1
                                              e0b
Cluster node2 clus1 169.254.47.194 node2
                                              e0a
Cluster node2 clus2 169.254.19.183 node2
                                              e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
cluster1::*> set -privilege admin
cluster1::*>
```

20. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

system cluster-switch log setup-password and system cluster-switch log enable-collection

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
\{y | n\}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

Replace a Cisco Nexus 92300YC switch

Replacing a defective Nexus 92300YC switch in a cluster network is a nondisruptive procedure (NDU).

Before you begin

The following conditions must exist before performing the switch replacement in the current environment and on the replacement switch.

- Existing cluster and network infrastructure:
 - The existing cluster must be verified as completely functional, with at least one fully connected cluster switch.
 - All cluster ports must be up.
 - All cluster logical interfaces (LIFs) must be up and on their home ports.
 - The ONTAP cluster ping-cluster -node node1 command must indicate that basic connectivity and larger than PMTU communication are successful on all paths.
- Nexus 92300YC replacement switch:
 - Management network connectivity on the replacement switch must be functional.
 - Console access to the replacement switch must be in place.
 - The node connections are ports 1/1 through 1/64.
 - All Inter-Switch Link (ISL) ports must be disabled on ports 1/65 and 1/66.
 - The desired reference configuration file (RCF) and NX-OS operating system image switch must be loaded onto the switch.
 - Initial customization of the switch must be complete, as detailed in:

Configuring a new Cisco Nexus 92300YC switch

Any previous site customizations, such as STP, SNMP, and SSH, should be copied to the new switch.

About this task

You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.

The examples in this procedure use the following switch and node nomenclature:

- The names of the existing Nexus 92300YC switches are cs1 and cs2.
- The name of the new Nexus 92300YC switch is newcs2.
- The node names are node1 and node2.
- The cluster ports on each node are named e0a and e0b.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The prompt for changes to all cluster nodes is cluster1::*>



The following procedure is based on the following cluster network topology:

Cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore

Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status

e0a false	Cluster	Cluster	up	9000	auto/10000	healthy
e0b false	Cluster	Cluster	up	9000	auto/10000	healthy
Node: nod	le2					
Ignore					Speed(Mbps)	Uool+b
Health					speed (Mbps)	nealth
Port Status	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster	up	9000	auto/10000	healthy
e0b false	Cluster	Cluster	up	9000	auto/10000	healthy
4 entries	s were display	red.				

<pre>cluster1::*></pre>	network	interface	show	-vserver	Cluster	
1	[0 0 1 0 0]	Ctatua	Mc	+		

	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	node1_clus1	l up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	2 up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	l up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	2 up/up	169.254.19.183/16	node2	e0b
true					
4 entries we	ere displaye	ed.			

cluster1::*> network device-discovery show -protocol cdp

Node/ Local Discovered

Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-
C92300YC				
	e0b	cs2	Eth1/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C92300YC				
	e0b	cs2	Eth1/1	N9K-
C92300YC				
1 antrias	ware die	anlaszed		

4 entries were displayed.

cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
node1	Eth1/1	144	Н	FAS2980	e0a
node2	Eth1/2	145	Н	FAS2980	e0a
cs2(FD0220329V5)	Eth1/65	176	R S I s	N9K-C92300YC	Eth1/65
cs2(FD0220329V5)	Eth1/66	176	RSIs	N9K-C92300YC	Eth1/66

Total entries displayed: 4

cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
node1	Eth1/1	139	Н	FAS2980	e0b
node2	Eth1/2	124	Н	FAS2980	e0b
cs1(FD0220329KU)	Eth1/65	178	R S I s	N9K-C92300YC	Eth1/65
cs1(FD0220329KU)	Eth1/66	178	RSIs	N9K-C92300YC	Eth1/66

Steps

1. Install the appropriate RCF and image on the switch, newcs2, and make any necessary site preparations.

If necessary, verify, download, and install the appropriate versions of the RCF and NX-OS software for the new switch. If you have verified that the new switch is correctly set up and does not need updates to the RCF and NX-OS software, continue to step 2.

- a. Go to the NetApp Cluster and Management Network Switches Reference Configuration File Description Page on the NetApp Support Site.
- b. Click the link for the *Cluster Network and Management Network Compatibility Matrix*, and then note the required switch software version.
- c. Click your browser's back arrow to return to the **Description** page, click **CONTINUE**, accept the license agreement, and then go to the **Download** page.
- d. Follow the steps on the Download page to download the correct RCF and NX-OS files for the version of ONTAP software you are installing.
- 2. On the new switch, log in as admin and shut down all of the ports that will be connected to the node cluster interfaces (ports 1/1 to 1/64).

If the switch that you are replacing is not functional and is powered down, go to Step 4. The LIFs on the cluster nodes should have already failed over to the other cluster port for each node.

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

3. Verify that all cluster LIFs have auto-revert enabled:

network interface show -vserver Cluster -fields auto-revert

```
cluster1::> network interface show -vserver Cluster -fields auto-revert
            Logical
            Interface
Vserver
                         Auto-revert
Cluster
            nodel clus1 true
Cluster
            node1 clus2 true
            node2 clus1
Cluster
                         true
            node2 clus2
Cluster
                         true
4 entries were displayed.
```

4. Verify that all the cluster LIFs can communicate:

```
cluster1::*> cluster ping-cluster node1
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e0a
Cluster node1 clus2 169.254.49.125 node1 e0b
Cluster node2 clus1 169.254.47.194 node2 e0a
Cluster node2 clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

5. Shut down the ISL ports 1/65 and 1/66 on the Nexus 92300YC switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/65-66
cs1(config-if-range)# shutdown
cs1(config-if-range)#
```

- 6. Remove all of the cables from the Nexus 92300YC cs2 switch, and then connect them to the same ports on the Nexus 92300YC newcs2 switch.
- 7. Bring up the ISLs ports 1/65 and 1/66 between the cs1 and newcs2 switches, and then verify the port channel operation status.

Port-Channel should indicate Po1(SU) and Member Ports should indicate Eth1/65(P) and Eth1/66(P).

This example enables ISL ports 1/65 and 1/66 and displays the port channel summary on switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config) # int e1/65-66
cs1(config-if-range) # no shutdown
cs1(config-if-range)# show port-channel summary
                  P - Up in port-channel (members)
Flags: D - Down
       I - Individual H - Hot-standby (LACP only)
       s - Suspended r - Module-removed
       b - BFD Session Wait
       S - Switched R - Routed
       U - Up (port-channel)
       p - Up in delay-lacp mode (member)
       M - Not in use. Min-links not met
Group Port- Type Protocol Member Ports
     Channel
1 Po1(SU) Eth LACP Eth1/65(P) Eth1/66(P)
cs1(config-if-range)#
```

8. Verify that port e0b is up on all nodes:

network port show ipspace Cluster

The output should be similar to the following:

cluster1:	:*> network p	ort show -:	ipspace	Clus	ter		
Node: node	e1						
Ignore						G L(M)	
Health						Speed (Mbps)	Health
	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
Node: nod	e2						
Ignore						Speed(Mbps)	Health
Health Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
e0a false	Cluster	Cluster		up	9000	auto/10000	healthy
e0b false	Cluster	Cluster		up	9000	auto/auto	-
4 entries	were display	ed.					

9. On the same node you used in the previous step, revert the cluster LIF associated with the port in the previous step by using the network interface revert command.

In this example, LIF node1_clus2 on node1 is successfully reverted if the Home value is true and the port is e0b.

The following commands return LIF node1_clus2 on node1 to home port e0a and displays information about the LIFs on both nodes. Bringing up the first node is successful if the Is Home column is true for both cluster interfaces and they show the correct port assignments, in this example e0a and e0b on node1.

cluster1::*	> network int	erface show	-vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true		/	160 054 40 105/16	1	- 01-
true	nodel_clus2	up/up	169.254.49.125/16	nodel	e0b
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true	node2_clus2	up/up	169.254.19.183/16	node2	e0a
false					
4 entries w	ere displayed				

10. Display information about the nodes in a cluster:

cluster show

This example shows that the node health for node1 and node2 in this cluster is true:

```
Cluster1::*> cluster show

Node Health Eligibility

-----
node1 false true
node2 true true
```

11. Verify that all physical cluster ports are up:

network port show ipspace Cluster

cluster1:	:*> network	port show -ipspace	Clust	er		
Node: nod	le1					
Ignore					2 1(17)	
Health					Speed (Mbps)	Health
	_	Broadcast Domain			Admin/Oper	Status
e0a false	Cluster	Cluster	up	9000	auto/10000	healthy
e0b false	Cluster	Cluster	up	9000	auto/10000	healthy
Node: nod	le2					
Ignore						
Health					Speed (Mbps)	Health
	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
e0a false	Cluster	Cluster	up	9000	auto/10000	healthy
	Cluster	Cluster	up	9000	auto/10000	healthy
4 entries	were displa	yed.				

12. Verify that all the cluster LIFs can communicate:

cluster ping-cluster

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1 clus1 169.254.209.69 node1 e0a
Cluster node1 clus2 169.254.49.125 node1 e0b
Cluster node2 clus1 169.254.47.194 node2 e0a
Cluster node2 clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
. . . .
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
. . . . . . . . . . . . . . . . . . .
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

13. Confirm the following cluster network configuration:

network port show

Ignore				Speed	d (Mbps	3)	Health
Health Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
	Cluster	Cluster		up	9000	auto/10000	healthy
false e0b false	Cluster	Cluster		up	9000	auto/10000	healthy
4 entries	were displa	yed.					
cluster1:	:*> network :	interface sh	ow -vse	rver	Clust	ter	
	_	Status	Networ	:k		Current	
Current Is Vserver Home	Interface	Admin/Oper					Port
Cluster	node1 clus	s1 up/up	169.25	54.20°	9.69/ ⁻	16 node1	e0a
true	_						
true	nodel_clu	s2 up/up	169.25	4.49.	. 125/.	16 node1	e0b
true	node2_clu	s1 up/up	169.25	4.47.	.194/1	16 node2	e0a
true	node2_clu	s2 up/up	169.25	4.19.	.183/1	16 node2	e0b
4 entries	were displa	yed.					
cluster1:	:> network d	evice-discov	ery sho	ıq- w	rotoco	ol cdp	
	Local Di		Chassis	;ID)	Inte	rface	Platform
							-
node2	/cdp	1			0 / 2		NOU
	e0a csi	L			0/2		N9K-
C92300YC							

C92300YC	/ 1					
	/cdp			0./1		
	e0a	csl		0/1	N9K	-
C92300YC						
	e0b	newcs2		0/1	N9K	-
C92300YC						
4 entries we	ere disp	olayed.				
cs1# show c d	lp neigh	nbors				
	7 - 1 · · · · ·	D			7 D	
Capability C		R - Router, T -				rıage
		S - Switch, H -				
		/ - VoIP-Phone,			ed-Device,	
	S	s - Supports-STI	P-Dispute			
Device-ID		Local Intrfce	n Uld+ma	Canabilit	Dlatform	
Port ID		LOCAL INCLICE	e niacile	Capabiliti	y Plation	
		D+b1 /1	1 / /		E7 C2000	- 0
node1		Eth1/1		H		e0
node2		Eth1/2				
newcs2 (FDO29)6348FU)	Eth1/65	176	RSIS	N9K-C92300Y	С
Eth1/65						
newcs2(FDO29)6348FU)	Eth1/66	176	R S I s	N9K-C92300Y	С
Eth1/66						
Total entrie	es displ	Layed: 4				
cs2# show c ơ	lp neigh	nbors				
cs2# show c d	lp neigh	nbors				
		nbors R - Router, T -	Trans-Br	idge, B - :	Source-Route-B	ridge
	Codes: F	R - Router, T -		-		ridge
	Codes: F	R - Router, T - S - Switch, H -	Host, I	- IGMP, r	- Repeater,	ridge
	Codes: F	R - Router, T - S - Switch, H - VoIP-Phone,	Host, I D - Remo	- IGMP, r · tely-Manage	- Repeater,	ridge
	Codes: F	R - Router, T - S - Switch, H -	Host, I D - Remo	- IGMP, r · tely-Manage	- Repeater,	ridge
Capability C	Codes: F	R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STE	Host, I D - Remo P-Dispute	- IGMP, r · tely-Manage	- Repeater, ed-Device,	_
Capability C	Codes: F	R - Router, T - S - Switch, H - VoIP-Phone,	Host, I D - Remo P-Dispute	- IGMP, r · tely-Manage	- Repeater, ed-Device,	_
Capability C Device-ID ID	Codes: F	R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STE	Host, I D - Remo P-Dispute Hldtme C	- IGMP, r · tely-Manage	- Repeater, ed-Device, Platform	Port
Capability C Device-ID ID node1	Codes: F	R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STE Local Intrfce Eth1/1	Host, I D - Remo P-Dispute Hldtme C	- IGMP, r tely-Manage	- Repeater, ed-Device, Platform FAS2980	Port
Capability C Device-ID ID node1 node2	Codes: F	R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STF Local Intrfce Eth1/1 Eth1/2	Host, I D - Remo P-Dispute Hldtme C 139 H 124 H	- IGMP, r tely-Manage	- Repeater, ed-Device, Platform FAS2980 FAS2980	Port
Device-ID ID node1 node2 cs1(FD022032	Codes: F	R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STF Local Intrfce Eth1/1 Eth1/2	Host, I D - Remo P-Dispute Hldtme C 139 H 124 H	- IGMP, r tely-Manage apability	- Repeater, ed-Device, Platform FAS2980	Port
Capability C Device-ID ID node1 node2	Codes: F	R - Router, T - S - Switch, H - V - VoIP-Phone, S - Supports-STF Local Intrfce Eth1/1 Eth1/2 Eth1/65	Host, I D - Remo P-Dispute Hldtme C 139 H 124 H	- IGMP, r tely-Manage	- Repeater, ed-Device, Platform FAS2980 FAS2980	Port

Eth1/66

Total entries displayed: 4

14. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using gthe commands:

 $\verb|system| cluster-switch| log| setup-password| \verb|and| system| cluster-switch| log| enable-collection|$

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? \{y|n\}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system cluster-switch log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



If any of these commands return an error, contact NetApp support.

NetApp CN1610 switches

NetApp CN1610 Switches

The CN1610 is a high bandwidth, managed Layer 2 switch that provides 16 10-Gigabit Small Form-Factor Pluggable Plus (SFP+) ports. The switch includes redundant power supplies and fan trays that support hot swapping for high availability.

This 1U switch can be installed in a standard 19-inch NetApp 42U system cabinet or third-party cabinet.

The switch supports local management through the console port or remote management by using Telnet or SSH through a network connection. The CN1610 includes a dedicated 1-Gigabit Ethernet RJ45 management port for out-of-band switch management. You can manage the switch by entering commands into the command-line interface (CLI) or by using an SNMP-based network management system (NMS).

Install FASTPATH software and RCFs on a NetApp cluster switch

You must install the FASTPATH software and reference configuration files (RCFs) on a NetApp CN1610 cluster switch.

Before you begin

- The cluster must be a fully functioning cluster.
- There must be no defective cluster network interface cards (NICs), and all connected ports on the cluster switch must be functional.
- All cluster ports must be up.
- · All cluster logical interfaces (LIFs) must be up and must not have been migrated.
- The ONTAP (privilege: advanced) cluster ping-cluster -node node1 command must indicate that larger than PMTU communication is successful on all paths.
- You must consult the switch compatibility table on the NetApp CN1601 and CN1610 Switches page for the supported FASTPATH, RCF, and ONTAP versions.

There can be command dependencies between command syntax in the RCF and FASTPATH versions.



In RCF version 1.2, support for Telnet has been explicitly disabled because of security concerns. To avoid connectivity issues while installing RCF 1.2, you must verify that Secure Shell (SSH) is enabled. The NetApp® CN1610 Switch Administrator's Guide has more information about SSH.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The procedures in this document use the clustered Data ONTAP 8.2 syntax. As a result, the cluster Vserver, LIF names, and CLI output will be different than those in Data ONTAP 8.3.
- The two NetApp switches are cs1 and cs2.
- The two cluster LIFs are clus1 and clus2.

- The Vservers are vs1 and vs2.
- The cluster::*> prompt indicates the name of the cluster.
- The cluster ports on each node are named e1a and e2a.

The Hardware Universe has more information about the actual cluster ports that are supported on your platform.

- The Inter-Switch Links (ISLs) that are supported for the NetApp cluster switch are ports 0/13 through 0/16.
- The node connections that are supported for the NetApp cluster switch are ports 0/1 through 0/12.

This procedure has two parts:

- Install FASTPATH software describes how to install the FASTPATH software.
- Install an RCF on a CN1610 switch describes how to install RCFs.

Install FASTPATH software

When you install the FASTPATH software on your NetApp switches, you must begin the upgrade with the second switch, *cs2*.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

2. Log into the switch as admin. There is no password by default. At the (cs2) # prompt, enter the enable command. Again, there is no password by default. This gives you access to Privileged EXEC mode, which allows you to configure the network interface.

```
(cs2) # enable
Password (Enter)
(cs2) #
```

3. On the console of each node, migrate clus2 to port e1a: network interface migrate

```
cluster::*> network interface migrate -vserver vs1 -lif clus2 -source
-node node1 -destnode node1 -dest-port e1a
cluster::*> network interface migrate -vserver vs2 -lif clus2 -source
-node node2 -destnode node2 -dest-port e1a
```

4. On the console of each node, verify that the migration took place: network interface show

The following example shows that clus2 has migrated to port e1a on both nodes:

cluster::*> network interface show -role cluster Logical Status Network Current Current Is Vserver Interface Admin/Open Address/Mask Node Port Home vs1 clus1 up/up 10.10.10.1/16 node1 ela true clus2 up/up 10.10.10.2/16 node1 ela false vs2 up/up 10.10.10.1/16 node2 clus1 e1a true up/up 10.10.10.2/16 node2 clus2 e1a false

5. Shut down cluster port e2a on both nodes: network port modify

The following example shows port e2a being shut down on both nodes:

```
cluster::*> network port modify -node node1 -port e2a -up-admin false
cluster::*> network port modify -node node2 -port e2a -up-admin false
```

6. Verify that port e2a is shut down on both nodes: network port show

cluste	r::*>	network :	port :	show -r	ole cluster		
Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

7. Shut down the Inter-Switch Link (ISL) ports on cs1, the active NetApp switch:

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

8. Back up the current active image on cs2.

```
Tmage Descriptions .

active:
backup:

Images currently available on Flash

unit active backup current-active next-active

1 1.1.0.3 1.1.0.1 1.1.0.3 1.1.0.3

(cs2) # copy active backup
Copying active to backup
Copy operation successful
(cs2) #
```

9. Download the image file to the switch.

Copying the image file to the active image means that when you reboot, that image establishes the running FASTPATH version. The previous image remains available as a backup.

10. Verify the running version of the FASTPATH software.

```
(cs2) # show version
Switch: 1
System Description..... Broadcom Scorpion 56820
                           Development System - 16 TENGIG,
                           1.1.0.3, Linux 2.6.21.7
Machine Type..... Broadcom Scorpion 56820
                           Development System - 16TENGIG
Machine Model..... BCM-56820
Serial Number..... 10611100004
FRU Number.....
Part Number..... BCM56820
Maintenance Level..... A
Burned In MAC Address................ 00:A0:98:4B:A9:AA
Software Version..... 1.1.0.3
Operating System..... Linux 2.6.21.7
Network Processing Device..... BCM56820 B0
Additional Packages..... FASTPATH QOS
                          FASTPATH IPv6 Management
```

11. View the boot images for the active and backup configuration.

```
(cs2) # show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash

unit active backup current-active next-active

1 1.1.0.3 1.1.0.3 1.1.0.3 1.1.0.5
```

12. Reboot the switch.

```
(cs2) \# reload

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

System will now restart!
```

13. Log in again, and verify the new version of the FASTPATH software.

```
(cs2) # show version
Switch: 1
System Description..... Broadcom Scorpion 56820
                        Development System - 16 TENGIG,
                        1.1.0.5, Linux 2.6.21.7
Machine Type..... Broadcom Scorpion 56820
                        Development System - 16TENGIG
Machine Model..... BCM-56820
Serial Number..... 10611100004
FRU Number.....
Part Number..... BCM56820
Maintenance Level..... A
Software Version..... 1.1.0.5
Operating System..... Linux 2.6.21.7
Network Processing Device..... BCM56820 B0
Additional Packages..... FASTPATH QOS
                        FASTPATH IPv6 Management
```

14. Bring up the ISL ports on cs1, the active switch.

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # no shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

15. Verify that the ISLs are operational: show port-channel 3/1

The Link State field should indicate Up.

```
(cs2) # show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr Device/
             Port
                   Port
Ports Timeout
             Speed
                   Active
0/13 actor/long
             10G Full True
   partner/long
0/14 actor/long
             10G Full True
   partner/long
0/15 actor/long
             10G Full True
   partner/long
0/16 actor/long 10G Full True
    partner/long
```

16. Copy the running-config file to the startup-config file when you are satisfied with the software versions and switch settings.

```
(cs2) # 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!
```

17. Enable the second cluster port, e2a, on each node: network port modify

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> **network port modify -node node2 -port e2a -up-admin true**
```

18. Revert clus2 that is associated with port e2a: network interface revert

The LIF might revert automatically, depending on your version of ONTAP software.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

19. Verify that the LIF is now home (true) on both nodes: network interface show -role cluster

```
cluster::*> network interface show -role cluster
       Logical Status Network Current Is
Vserver Interface Admin/Oper Address/Mask Node Port Home
vs1
       clus1 up/up 10.10.10.1/24 node1 ela true
                        10.10.10.2/24 node1 e2a
       clus2
               up/up
                                                 true
vs2
       clus1
               up/up
                        10.10.10.1/24 node2 e1a
                                                 true
                up/up
                        10.10.10.2/24 node2 e2a
       clus2
                                                  true
```

20. View the status of the nodes: cluster show

- 21. Repeat step 1 through step 18 to upgrade the FASTPATH software on the other switch, cs1.
- 22. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Install a Reference Configuration File on a CN1610 switch

When you are installing a reference configuration file (RCF), you must first migrate the cluster LIFs away from switch cs2. After the RCF is installed and validated, the LIFs can be migrated back.

Before you begin

You must have saved the configuration that is currently running on your switch.

Steps

1. Save your current switch configuration information: write memory

The following example shows the current switch configuration being saved to the startup configuration (startup-config) file on switch cs2:

```
(cs2) # 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!
```

2. On the console of each node, migrate clus2 to port e1a: network interface migrate

```
cluster::*> network interface migrate -vserver vs1 -lif clus2 -source
-node node1 -destnode node1 -dest-port e1a

cluster::*> network interface migrate -vserver vs2 -lif clus2 -source
-node node2 -destnode node2 -dest-port e1a
```

3. On the console of each node, verify that the migration occurred: network interface show -role cluster

The following example shows that clus2 has migrated to port e1a on both nodes:

```
cluster::*> network port show -role cluster
    clus1     up/up     10.10.10.1/16     node2     e1a     true
        clus2     up/up     10.10.10.2/16     node2     e1a     false
```

4. Shut down port e2a on both nodes: network port modify

The following example shows port e2a being shut down on both nodes:

```
cluster::*> network port modify -node node1 -port e2a -up-admin false
cluster::*> network port modify -node node2 -port e2a -up-admin false
```

5. Verify that port e2a is shut down on both nodes: network port show

cluster::*> network port show -role cluster							
Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

6. Shut down the ISL ports on cs1, the active NetApp switch.

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (interface 0/13-0/16) # shutdown
(cs1) (interface 0/13-0/16) # exit
(cs1) (config) # exit
```

7. Copy the RCF to the switch.



You must set the .scr extension as part of the file name before invoking the script. This extension is the extension for the FASTPATH operating system.

The switch will validate the script automatically as it is downloaded to the switch, and the output will go to the console.

```
(cs2) # copy tftp://10.10.0.1/CN1610_CS_RCF_v1.1.txt nvram:script
CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```

8. Verify that the script was downloaded and saved with the file name that you gave it.

9. Validate the script.



The script is validated during the download to verify that each line is a valid switch command line.

```
(cs2) # script validate CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script 'CN1610_CS_RCF_v1.1.scr' validated.
```

10. Apply the script to the switch.

```
(cs2) #script apply CN1610_CS_RCF_v1.1.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.1.scr' applied.
```

11. Verify that your changes have been implemented on the switch.

```
(cs2) # show running-config
```

The example displays the running-config file on the switch. You must compare the file to the RCF to verify that the parameters that you set are as you expect.

- 12. Save the changes.
- 13. Set the running-config file to be the standard one.

```
(cs2) # 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.
```

14. Reboot the switch and verify that the running-config file is correct.

After the reboot completes, you must log in, view the running-config file, and then look for the description on interface 3/64, which is the version label for the RCF.

```
(cs2) # reload
The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

15. Bring up the ISL ports on cs1, the active switch.

```
(cs1) # configure
(cs1) (config)# interface 0/13-0/16
(cs1) (Interface 0/13-0/16)# no shutdown
(cs1) (Interface 0/13-0/16)# exit
(cs1) (config)# exit
```

16. Verify that the ISLs are operational: show port-channel 3/1

The Link State field should indicate Up.

```
(cs2) # show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr Device/ Port Port
Ports Timeout
            Speed
                   Active
0/13 actor/long 10G Full True
   partner/long
0/14 actor/long 10G Full True
   partner/long
0/15 actor/long 10G Full True
   partner/long
0/16 actor/long 10G Full True
    partner/long
```

17. Bring up cluster port e2a on both nodes: network port modify

The following example shows port e2a being brought up on node1 and node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

18. Verify that port e2a is up on both nodes: network port show -role cluster

```
Cluster::*> network port show -role cluster

Auto-Negot Duplex Speed (Mbps)

Node Port Role Link MTU Admin/Oper Admin/Oper Admin/Oper

node1

ela cluster up 9000 true/true full/full auto/10000
e2a cluster up 9000 true/true full/full auto/10000

node2

ela cluster up 9000 true/true full/full auto/10000
e2a cluster up 9000 true/true full/full auto/10000
e2a cluster up 9000 true/true full/full auto/10000
```

19. On both nodes, revert clus2 that is associated with port e2a: network interface revert

The LIF might revert automatically, depending on your version of ONTAP.

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

20. Verify that the LIF is now home (true) on both nodes: network interface show -role cluster

```
cluster::*> network interface show -role cluster
      Logical Status Network Current Is
Vserver Interface Admin/Oper Address/Mask Node Port Home
vs1
     clus1 up/up 10.10.10.1/24 node1 ela true
      clus2
             up/up
                      10.10.10.2/24 node1
                                         e2a
                                               true
vs2
      clus1 up/up 10.10.10.1/24 node2 e1a
                                                true
              up/up
                     10.10.10.2/24 node2
      clus2
                                          e2a
                                                true
```

21. View the status of the node members: cluster show

22. Copy the running-config file to the startup-config file when you are satisfied with the software versions and switch settings.

```
(cs2) # 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!
```

23. Repeat step 1 through step 22 to upgrade the RCF on the other switch, cs1.

Related information

NetApp Support

Install FASTPATH software and RCFs on NetApp cluster switches running ONTAP 8.3.1 and later

The installation steps are the same for both NetApp CN1601 management switches and CN1610 cluster switches running ONTAP 8.3.1 or later. However, the two models require different software and RCFs.

Before you begin

- The cluster must be a fully functioning cluster.
- There must be no defective cluster NICs, and all connected ports on both cluster switches must be functional.
- All cluster ports must be up.
- All cluster logical interfaces (LIFs) must be up and must not have been migrated.
- The ONTAP (privilege: advanced) cluster ping-cluster -node node1 command must indicate that larger than PMTU communication is successful on all paths.
- You must be using supported FASTPATH, RCF, and ONTAP versions.

There can be command dependencies between command syntax in the RCF and FASTPATH versions. The switch compatibility page lists the supported versions. See NetApp CN1601 and CN1610 Switches for details.

About this task

The examples in this procedure use the following switch and node nomenclature:

- The two NetApp switch names are cs1 and cs2.
- The cluster logical interface (LIF) names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The storage virtual machine (SVM) name is Cluster.
- The cluster1::*> prompt indicates the name of the cluster.

• The cluster ports on each node are named e0a and e0b.

The Hardware Universe contains the actual cluster ports supported on your platform.

- The Inter-Switch Links (ISLs) supported for the NetApp cluster switches are ports 0/13 through 0/16.
- The node connections supported for the NetApp cluster switches are ports 0/1 through 0/12.
- The example in this procedure begins the upgrade on the second switch, cs2.
- The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.
- The examples and outputs might vary depending on different releases of FASTPATH, RCF, and ONTAP.

Steps

1. Display information about the network ports on the cluster:

```
network port show -ipspace cluster
```

The following example shows the type of output from the command:

cluste	r1::> netwo	ork port show	-ipspace cluster			
						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link N	UTU	Admin/Oper
node1						
	e0a	Cluster	Cluster	up	9000	auto/10000
	e0b	Cluster	Cluster	up	9000	auto/10000
node2						
	e0a	Cluster	Cluster	up	9000	auto/10000
	e0b	Cluster	Cluster	up	9000	auto/10000
4 entr	ies were d	isplayed.				

2. Display information about the LIFs on the cluster:

```
network interface show -role cluster
```

The following example shows the logical interfaces on the cluster. In this example the -role parameter displays information about the LIFs that are associated with cluster ports:

(network	interface sl	now)			
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
	_				
Cluster					
	node1_clus	l up/up	10.254.66.82/16	node1	e0a
true					
	node1_clus	2 up/up	10.254.206.128/16	node1	e0b
true					
	node2_clus	l up/up	10.254.48.152/16	node2	e0a
true					
	node2_clus	2 up/up	10.254.42.74/16	node2	e0b
true					

3. On each respective node, using a node management LIF, migrate node1_clus2 to e0a on node1 and node2 clus2 to e0a on node2:

network interface migrate

You must enter the commands on the controller consoles that own the respective cluster LIFs.

```
cluster1::> network interface migrate -vserver Cluster -lif node1_clus2
-destination-node node1 -destination-port e0a
cluster1::> network interface migrate -vserver Cluster -lif node2_clus2
-destination-node node2 -destination-port e0a
```



For this command, the name of the cluster is case-sensitive and the command should be run on each node. It is not possible to run this command in the general cluster LIF.

4. Verify that the migration took place by using the network interface show command on a node.

The following example shows that clus2 has migrated to port e0a on nodes node1 and node2:

cluster1::>	**network in	terface sh	now -role cluster*	+	
	Logical S	tatus	Network	Current	
Current Is					
Vserver	Interface A	.dmin/Oper	Address/Mask	Node	Port
Home					
	_				
Cluster					
	nodel_clus1	up/up	10.254.66.82/16	node1	e0a
true					
	node1_clus2	up/up	10.254.206.128/16	node1	e0a
false					
	node2_clus1	up/up	10.254.48.152/16	node2	e0a
true					
	node2_clus2	up/up	10.254.42.74/16	node2	e0a
false					
4 entries we	ere displayed	. •			

5. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

6. Shut down cluster port e0b on both nodes:

```
network port modify -node node_name -port port_name -up-admin false
```

You must enter the commands on the controller consoles that own the respective cluster LIFs.

The following example shows the commands to shut down port e0b on all nodes:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin false
cluster1::*> network port modify -node node2 -port e0b -up-admin false
```

7. Verify that port e0b is shut down on both nodes:

network port show

cluste	<pre>cluster1::*> network port show -role cluster</pre>						
						Speed	
(Mbps)							
Node	Port	IPspace	Broadcast Domain	Link M	ITU	Admin/Oper	
node1							
	e0a	Cluster	Cluster	up	9000	auto/10000	
	e0b	Cluster	Cluster	down	9000	auto/10000	
node2							
	e0a	Cluster	Cluster	up	9000	auto/10000	
	e0b	Cluster	Cluster	down	9000	auto/10000	
4 entr	ies were di	isplayed.					

8. Shut down the Inter-Switch Link (ISL) ports on cs1.

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

9. Back up the current active image on cs2.

Image Descriptions

active:
backup:

Images currently available on Flash

unit active backup current-active next-active

1 1.1.0.5 1.1.0.3 1.1.0.5 1.1.0.5

(cs2) # copy active backup
Copying active to backup
Copy operation successful

10. Verify the running version of the FASTPATH software.

(cs2) # show version	
Switch: 1	
System DescriptionLinux	NetApp CN1610, 1.1.0.5,
	2.6.21.7
Machine Type. Machine Model. Serial Number. Burned In MAC Address Software Version.	CN1610 20211200106 00:A0:98:21:83:69 1.1.0.5
Operating System	
Network Processing Device Part Number	_
More or (q)uit	
Additional Packages	FASTPATH QOS FASTPATH IPv6 Management

11. Download the image file to the switch.

Copying the image file to the active image means that when you reboot, that image establishes the running FASTPATH version. The previous image remains available as a backup.

12. Confirm the current and next-active boot image versions:

show bootvar

```
(cs2) #show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash

unit active backup current-active next-active

1 1.1.0.8 1.1.0.8 1.1.0.8 1.2.0.7
```

13. Install the compatible RCF for the new image version to the switch.

If the RCF version is already correct, skip to step 18 to bring up the ISL ports.

```
(cs2) #copy tftp://10.22.201.50//CN1610 CS RCF v1.2.txt nvram:script
CN1610 CS RCF v1.2.scr
Mode..... TFTP
Path...../
Filename..... CN1610 CS RCF v1.2.txt
Data Type..... Config Script
Destination Filename..... CN1610 CS RCF v1.2.scr
File with same name already exists.
WARNING: Continuing with this command will overwrite the existing file.
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
Validating configuration script...
[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```



The .scr extension must be set as part of the file name before invoking the script. This extension is for the FASTPATH operating system.

The switch validates the script automatically as it is downloaded to the switch. The output goes to the console.

14. Verify that the script was downloaded and saved to the file name you gave it.

15. Apply the script to the switch.

```
(cs2) #script apply CN1610_CS_RCF_v1.2.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.2.scr' applied.
```

16. Verify that the changes have been applied to the switch, and then save them:

show running-config

```
(cs2) #show running-config
```

17. Save the running configuration so it becomes the startup configuration when you reboot the switch.

```
(cs2) #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!
```

18. Reboot the switch.

```
(cs2) #reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

19. Log in again, and then verify that the switch is running the new version of the FASTPATH software.

```
(cs2) #show version
Switch: 1
System Description..... NetApp CN1610,
1.2.0.7, Linux
                         3.8.13-4ce360e8
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Software Version..... 1.2.0.7
Operating System..... Linux 3.8.13-4ce360e8
Network Processing Device..... BCM56820 B0
Part Number..... 111-00893
CPLD version......0x5
Additional Packages..... FASTPATH QOS
                         FASTPATH IPv6 Management
```

After the reboot completes, you must log in to verify the image version, view the running configuration, and look for the description on interface 3/64, which is the version label for the RCF.

20. Bring up the ISL ports on cs1, the active switch.

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #no shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

21. Verify that the ISLs are operational:

```
show port-channel 3/1
```

The Link State field should indicate Up.

```
(cs1) #show port-channel 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
(Enhanced hashing mode)
Mbr Device/
           Port
                 Port
Ports Timeout
           Speed
                 Active
0/13 actor/long
           10G Full True
   partner/long
0/14 actor/long
           10G Full True
   partner/long
   actor/long
0/15
           10G Full False
   partner/long
   actor/long 10G Full True
0/16
    partner/long
```

22. Bring up cluster port e0b on all nodes:

```
network port modify
```

You must enter the commands on the controller consoles that own the respective cluster LIFs.

The following example shows port e0b being brought up on node1 and node2:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin true
cluster1::*> network port modify -node node2 -port e0b -up-admin true
```

23. Verify that the port e0b is up on all nodes:

```
network port show -ipspace cluster
```

<pre>cluster1::*> network port show -ipspace cluster</pre>								
						Speed		
(Mbps)								
Node	Port	IPspace	Broadcast Don	nain Link	MTU	Admin/Oper		
node1								
	e0a	Cluster	Cluster	up	9000	auto/10000		
	e0b	Cluster	Cluster	up	9000	auto/10000		
node2								
	e0a	Cluster	Cluster	up	9000	auto/10000		
	e0b	Cluster	Cluster	up	9000	auto/10000		
4 entries were displayed.								

24. Verify that the LIF is now home (true) on both nodes:

network interface show -role cluster

<pre>cluster1::*> network interface show -role cluster</pre>								
	Logical	Status	Network	Current				
Current Is								
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port			
Home								
Cluster								
	node1_clus1	L up/up	169.254.66.82/16	node1	e0a			
true								
	node1_clus2	2 up/up	169.254.206.128/16	node1	e0b			
true								
	node2_clus1	L up/up	169.254.48.152/16	node2	e0a			
true								
	node2_clus2	2 up/up	169.254.42.74/16	node2	e0b			
true								
4 entries were displayed.								

25. Show the status of the node members:

cluster show

```
Node Health Eligibility Epsilon
-----
node1 true true false
node2 true true false
2 entries were displayed.
```

26. Return to the admin privilege level:

```
set -privilege admin
```

27. Repeat the steps 1 through 18 to upgrade the FASTPATH software and RCF on the other switch, cs1.

If you	Then
Do not need to install the RCF	Go to Step 18 to finish the installation.
Need to install the RCF	Go to Step 13.

Migrate to a two-node switched cluster with NetApp CN1610 cluster switches

If you have a two-node switchless cluster, you can migrate, non-disruptively, to a two-node switched cluster that includes NetApp CN1610 cluster-network switches. The procedure you use depends on whether you have two dedicated cluster-network ports on each controller or a single cluster port on each controller.

About this task

Most systems require two dedicated cluster-network ports on each controller.

FAS22xx nodes allow a single cluster port on each controller.

There are two migration options available:

- Migrate from a switchless cluster to a switched NetApp CN1610 cluster environment
- Migrate from a switchless cluster (FAS22xx systems with a single cluster-network connection)

Migrate from a switchless cluster environment to a switched NetApp CN1610 cluster environment

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using CN1610 cluster network switches that enables you to scale beyond two nodes.

Before you begin

Two-node switchless configuration:

- The two-node switchless configuration must be properly set up and functioning.
- The nodes must be running ONTAP 8.2 or later.
- All cluster ports must be in the up state.
- All cluster logical interfaces (LIFs) must be in the up state and on their home ports.

CN1610 cluster switch configuration:

- The CN1610 cluster switch infrastructure must be and fully functional on both switches.
- · Both switches must have management network connectivity.
- There must be console access to the cluster switches.
- CN1610 node-to-node switch and switch-to-switch connections must use twinax or fiber cables.

The Hardware Universe contains more information about cabling.

- Inter-Switch Link (ISL) cables must be connected to ports 13 through 16 on both CN1610 switches.
- Initial customization of both the CN1610 switches must be completed.

Any previous site customization, such as SMTP, SNMP, and SSH should be copied to the new switches.

About this task

The examples in this procedure use the following cluster switch and node nomenclature:

- The names of the CN1610 switches are cs1 and cs2.
- The names of the LIFs are clus1 and clus2.
- The names of the nodes are node1 and node2.
- The cluster::*> prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e1a and e2a.

The Hardware Universe contains the latest information about the actual cluster ports for your platforms.

Steps

 Change the privilege level to advanced, entering y when prompted to continue: set -privilege advanced

The advanced prompt (*>) appears.

2. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh

x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster::*> system node autosupport invoke -node * -type all -message
MAINT=2h
```

3. Disable all of the node-facing ports (not ISL ports) on both the new cluster switches cs1 and cs2.

You must not disable the ISL ports.

The following example shows that node-facing ports 1 through 12 are disabled on switch cs1:

```
(cs1)> enable
(cs1)# configure
(cs1) (Config)# interface 0/1-0/12
(cs1) (Interface 0/1-0/12)# shutdown
(cs1) (Interface 0/1-0/12)# exit
(cs1) (Config)# exit
```

The following example shows that node-facing ports 1 through 12 are disabled on switch cs2:

```
(c2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/12
(cs2) (Interface 0/1-0/12)# shutdown
(cs2) (Interface 0/1-0/12)# exit
(cs2) (Config)# exit
```

4. Verify that the ISL and the physical ports on the ISL between the two CN1610 cluster switches cs1 and cs2 are up: show port-channel

The following example shows that the ISL ports are up on switch cs1:

```
(cs1) # show port-channel 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr
    Device/
             Port
                   Port
Ports Timeout
             Speed
                   Active
0/13 actor/long
             10G Full True
   partner/long
0/14 actor/long
            10G Full True
   partner/long
             10G Full True
0/15 actor/long
   partner/long
0/16
    actor/long
             10G Full True
    partner/long
```

The following example shows that the ISL ports are up on switch cs2:

```
(cs2) # show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
    Device/
Mbr
             Port
                    Port
Ports Timeout
             Speed
                    Active
_____
0/13 actor/long
             10G Full True
    partner/long
0/14 actor/long
             10G Full True
    partner/long
0/15
   actor/long
             10G Full True
    partner/long
0/16
   actor/long
             10G Full True
    partner/long
```

5. Display the list of neighboring devices: show isdp neighbors

This command provides information about the devices that are connected to the system.

The following example lists the neighboring devices on switch cs1:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
               S - Switch, H - Host, I - IGMP, r - Repeater
Device ID
                   Intf Holdtime Capability Platform
Port ID
cs2
                   0/13
                              11 S
                                                 CN1610
0/13
cs2
                   0/14
                              11
                                      S
                                                 CN1610
0/14
cs2
                   0/15
                              11
                                      S
                                                 CN1610
0/15
cs2
                   0/16
                              11
                                      S
                                                 CN1610
0/16
```

The following example lists the neighboring devices on switch cs2:

(cs2) # show isdp Capability Codes:	R - Router, T -			- ·
D ' TD	S - Switch, H -		-	
Device ID	Inti	Holatime	Capability	Platiorm
Port ID				
cs1	0/13	11	S	CN1610
0/13				
cs1	0/14	11	S	CN1610
0/14				
cs1	0/15	11	S	CN1610
0/15				
cs1	0/16	11	S	CN1610
0/16				

6. Display the list of cluster ports: network port show

The following example shows the available cluster ports:

Ignore					Speed(Mbps)	Health
Health						
Port Status	IPspace	Broadcast Domai	n Link	MTU	Admin/Oper	Status
	Q1 .			0.000	/10000	1 7.1
e0a false	Cluster	Cluster	up	9000	auto/10000	nealthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy
false	Q1			0000		11+1
e0c false	Cluster	Cluster	up	9000	auto/10000	neartny
e0d	Cluster	Cluster	up	9000	auto/10000	healthy
false e4a	Cluster	Cluster	110	9000	auto/10000	heal+h;
e4a false	Clustel	CIUSCEL	up	9000	aut0/10000	Hearthy
	Cluster	Cluster	up	9000	auto/10000	healthy
e4b false	Cluster	Cluster	ир	9000	auto/10000	healthy
false		Cluster	ир	9000	auto/10000	healthy
false Node: no		Cluster	ир	9000	auto/10000	healthy
false		Cluster	up	9000	auto/10000 Speed(Mbps)	
false Node: no Ignore Health	de2				Speed(Mbps)	Health
false Node: no Ignore Health Port	de2	Cluster Broadcast Domai			Speed(Mbps)	Health
false Node: no Ignore	de2				Speed(Mbps)	Health
false Node: no Ignore Health Port Status	de2 IPspace	Broadcast Domai	n Link	MTU	Speed(Mbps) Admin/Oper	Health Status
false Node: no Ignore Health Port	de2			MTU	Speed(Mbps)	Health Status
false Node: no Ignore Health Port Status e0a false e0b	de2 IPspace	Broadcast Domai	n Link	MTU 9000	Speed(Mbps) Admin/Oper	Health Status healthy
false Node: no Ignore Health Port Status e0a false e0b false	de2 IPspace Cluster Cluster	Broadcast Domai	n Link up up	MTU 9000 9000	Speed(Mbps) Admin/Operauto/10000 auto/10000	Health Status healthy healthy
false Node: no Ignore Health Port Status e0a false e0b	de2 IPspace Cluster	Broadcast Domai	n Link up	MTU 9000	Speed(Mbps) Admin/Operauto/10000 auto/10000	Health Status healthy healthy
false Node: no Ignore Health Port Status e0a false e0b false e0c false e0c	de2 IPspace Cluster Cluster	Broadcast Domai	n Link up up	MTU 9000 9000	Speed (Mbps) Admin/Oper auto/10000 auto/10000 auto/10000	Health Status healthy healthy
false Node: no Ignore Health Port Status e0a false e0b false e0c false e0d false	de2 IPspace Cluster Cluster Cluster Cluster Cluster	Broadcast Domai Cluster Cluster Cluster Cluster Cluster	n Link up up up	MTU 9000 9000 9000	Speed (Mbps) Admin/Oper auto/10000 auto/10000 auto/10000 auto/10000	Health Status healthy healthy healthy
false Node: no Ignore Health Port Status e0a false e0b false e0c false e0d	de2 IPspace Cluster Cluster Cluster Cluster	Broadcast Domai Cluster Cluster Cluster Cluster	n Link up up	MTU 9000 9000	Speed (Mbps) Admin/Oper auto/10000 auto/10000 auto/10000 auto/10000	Health Status healthy healthy healthy

7. Verify that each cluster port is connected to the corresponding port on its partner cluster node: run * cdpd show-neighbors

The following example shows that cluster ports e1a and e2a are connected to the same port on their cluster partner node:

	er::*> run * cdpc				
2 enti	ries were acted o	on.			
Node:	node1				
		Remote	Remote	Hold	
Remote		Kemote	remoce	11014	
		Interface	Platform	Time	
Capaba	lity				
_	·				
e1a	node2	e1a	FAS3270	137	Н
e2a	node2	e2a	FAS3270	137	Н
NT1	1 . 0				
Node:	nodez				
Local	Remote	Remote	Remote	Hold	
Remote					
Port	Device	Interface	Platform	Time	
Capab	lity				
		ela	FAS3270	161	Н
e2a	node1	e2a	FAS3270	161	Н

8. Verify that all of the cluster LIFs are up and operational: network interface show -vserver Cluster

Each cluster LIF should display true in the "Is Home" column.

	Logical	Status	Network	Current	Current Is
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2		,			
	clus1	up/up	10.10.11.1/16	node2	e1a
true	1 0	,	10 10 11 0/16	1 0	
t	Clus2	up/up	10.10.11.2/16	noae2	e2a
true					



The following modification and migration commands in steps 10 through 13 must be done from the local node.

9. Verify that all cluster ports are up: network port show -ipspace Cluster

cluste	r::*> n	etwork port s	how -i _l	pspace	Cluster		
					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
node1							
	e1a	clus1	up	9000	true/true	full/full	auto/10000
	e2a	clus2	up	9000	true/true	full/full	auto/10000
node2							
	e1a	clus1	up	9000	true/true	full/full	auto/10000
	e2a	clus2	up	9000	true/true	full/full	auto/10000
4		- 44 1 d					
4 entr	ies wer	e displayed.					

10. Set the -auto-revert parameter to false on cluster LIFs clus1 and clus2 on both nodes: network interface modify

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```



For release 8.3 and later, use the following command: network interface modify -vserver Cluster -lif * -auto-revert false

- 11. Ping the cluster ports to verify the cluster connectivity: cluster ping-cluster local
 - The command output shows connectivity between all of the cluster ports.
- 12. Migrate clus1 to port e2a on the console of each node: network interface migrate

The following example shows the process for migrating clus1 to port e2a on node1 and node2:

```
cluster::*> network interface migrate -vserver node1 -lif clus1 -source
-node node1 -dest-node node1 -dest-port e2a
cluster::*> network interface migrate -vserver node2 -lif clus1 -source
-node node2 -dest-node node2 -dest-port e2a
```



For release 8.3 and later, use the following command: network interface migrate -vserver Cluster -lif clus1 -destination-node node1 -destination -port e2a

13. Verify that the migration took place: network interface show -vserver Cluster

The following example verifies that clus1 is migrated to port e2a on node1 and node2:

cluster::*>	network in	terface s	how -vserver Clu	ster	
	Logical	Status	Network	Current	Current Is
Vserver	Interface	Admin/Op	er Address/Mask	Node	Port
Home					
node1	7 4	,	10 10 10 1/16		
C 1	clus1	up/up	10.10.10.1/16	node1	e2a
false	ala?	/	10.10.10.2/16	node1	e2a
true	clus2	up/up	10.10.10.2/16	nodei	eza
node2					
110002	clus1	up/up	10.10.11.1/16	node2	e2a
false	01401	αρ/ αρ	10.10.11.17.10	110002	024
	clus2	up/up	10.10.11.2/16	node2	e2a
true					
4 entries w	ere display	red.			

14. Shut down cluster port e1a on both nodes: network port modify

The following example shows how to shut down the port e1a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin false
cluster::*> network port modify -node node2 -port e1a -up-admin false
```

15. Verify the port status: network port show

The following example shows that port e1a is down on node1 and node2:

```
cluster::*> network port show -role cluster
                                  Auto-Negot Duplex
                                                       Speed
(Mbps)
                              MTU Admin/Oper Admin/Oper Admin/Oper
Node
     Port
            Role
                        Link
node1
      ela clus1
                       down 9000 true/true full/full
                                                        auto/10000
      e2a clus2
                              9000 true/true full/full
                                                        auto/10000
                       up
node2
                        down 9000 true/true full/full
                                                        auto/10000
      ela clus1
                             9000 true/true full/full
                                                        auto/10000
      e2a
           clus2
                        up
4 entries were displayed.
```

16. Disconnect the cable from cluster port e1a on node1, and then connect e1a to port 1 on cluster switch cs1, using the appropriate cabling supported by the CN1610 switches.

The Hardware Universe contains more information about cabling.

- 17. Disconnect the cable from cluster port e1a on node2, and then connect e1a to port 2 on cluster switch cs1, using the appropriate cabling supported by the CN1610 switches.
- 18. Enable all of the node-facing ports on cluster switch cs1.

The following example shows that ports 1 through 12 are enabled on switch cs1:

```
(cs1) # configure
(cs1) (Config) # interface 0/1-0/12
(cs1) (Interface 0/1-0/12) # no shutdown
(cs1) (Interface 0/1-0/12) # exit
(cs1) (Config) # exit
```

19. Enable the first cluster port e1a on each node: network port modify

The following example shows how to enable the port e1a on node1 and node2:

```
cluster::*> network port modify -node node1 -port ela -up-admin true
cluster::*> network port modify -node node2 -port ela -up-admin true
```

20. Verify that all of the cluster ports are up: network port show -ipspace Cluster

The following example shows that all of the cluster ports are up on node1 and node2:

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
node1							
	e1a	clus1	up	9000	true/true	full/full	auto/10000
	e2a	clus2	up	9000	true/true	full/full	auto/10000
node2							
	e1a	clus1	up	9000	true/true	full/full	auto/10000
	e2a	clus2	up	9000	true/true	full/full	auto/10000

21. Revert clus1 (which was previously migrated) to e1a on both nodes: network interface revert

The following example shows how to revert clus1 to the port e1a on node1 and node2:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```



For release 8.3 and later, use the following command: network interface revert -vserver Cluster -lif <nodename clus<N>>

22. Verify that all of the cluster LIFs are up, operational, and display as true in the "Is Home" column: network interface show -vserver Cluster

The following example shows that all of the LIFs are up on node1 and node2 and that the "Is Home" column results are true:

cluster::*>	network in	terface s	how -vserver Clu	ster	
	Logical	Status	Network	Current	Current Is
Vserver	Interface	Admin/Op	er Address/Mask	Node	Port
Home					
node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2		,			_
	clus1	up/up	10.10.11.1/16	node2	e1a
true		,	10 10 11 0/16		2
	clus2	up/up	10.10.11.2/16	node2	e2a
true					
4 entries w	ere display	ed.			

23. Display information about the status of the nodes in the cluster: cluster show

The following example displays information about the health and eligibility of the nodes in the cluster:

24. Migrate clus2 to port e1a on the console of each node: network interface migrate

The following example shows the process for migrating clus2 to port e1a on node1 and node2:

```
cluster::*> network interface migrate -vserver node1 -lif clus2 -source
-node node1 -dest-node node1 -dest-port e1a
cluster::*> network interface migrate -vserver node2 -lif clus2 -source
-node node2 -dest-node node2 -dest-port e1a
```



For release 8.3 and later, use the following command: network interface migrate -vserver Cluster -lif node1_clus2 -dest-node node1 -dest-port e1a

25. Verify that the migration took place: network interface show -vserver Cluster

The following example verifies that clus2 is migrated to port e1a on node1 and node2:

cluster::*>	network in	terface sh	now -vserver Clu	ster	
	Logical	Status	Network	Current	Current Is
Vserver	Interface	Admin/Ope	er Address/Mask	Node	Port
Home					
node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true		,			
	clus2	up/up	10.10.10.2/16	node1	e1a
false					
node2		/	10 10 11 1/16	1 0	4
	clus1	up/up	10.10.11.1/16	node2	e1a
true	al.,a2	/	10.10.11.2/16	~ ~ d ~ ?	010
false	clus2	up/up	10.10.11.2/10	node2	e1a
Talse					
4 entries w	ere display	ed			
1 CHCLICS W	cic dispidy	· .			

26. Shut down cluster port e2a on both nodes: network port modify

The following example shows how to shut down the port e2a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin false
cluster::*> network port modify -node node2 -port e2a -up-admin false
```

27. Verify the port status: network port show

The following example shows that port e2a is down on node1 and node2:

```
cluster::*> network port show -role cluster
                                  Auto-Negot Duplex
                                                      Speed
(Mbps)
                       Link MTU Admin/Oper Admin/Oper Admin/Oper
Node
     Port
            Role
node1
      ela clus1
                      up
                             9000 true/true full/full
                                                       auto/10000
      e2a clus2
                       down 9000 true/true full/full
                                                       auto/10000
node2
                             9000 true/true full/full auto/10000
      ela clus1
                       up
                        down 9000 true/true full/full
                                                       auto/10000
      e2a
           clus2
4 entries were displayed.
```

- 28. Disconnect the cable from cluster port e2a on node1, and then connect e2a to port 1 on cluster switch cs2, using the appropriate cabling supported by the CN1610 switches.
- 29. Disconnect the cable from cluster port e2a on node2, and then connect e2a to port 2 on cluster switch cs2, using the appropriate cabling supported by the CN1610 switches.
- 30. Enable all of the node-facing ports on cluster switch cs2.

The following example shows that ports 1 through 12 are enabled on switch cs2:

```
(cs2) # configure
(cs2) (Config) # interface 0/1-0/12
(cs2) (Interface 0/1-0/12) # no shutdown
(cs2) (Interface 0/1-0/12) # exit
(cs2) (Config) # exit
```

31. Enable the second cluster port e2a on each node:

The following example shows how to enable the port e2a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

32. Verify that all of the cluster ports are up: network port show -ipspace Cluster

The following example shows that all of the cluster ports are up on node1 and node2:

cluste	r::*>	network port	show -i		e Cluster Auto-Negot	Duplex	Speed
(Mbps)					2	-	-
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
node1							
	e1a	clus1	up	9000	true/true	full/full	auto/10000
	e2a	clus2	up	9000	true/true	full/full	auto/10000
node2							
	e1a	clus1	up	9000	true/true	full/full	auto/10000
	e2a	clus2	up	9000	true/true	full/full	auto/10000
4 entr	ies we	re displayed	•				

33. Revert clus2 (which was previously migrated) to e2a on both nodes: network interface revert

The following example shows how to revert clus2 to the port e2a on node1 and node2:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

For release 8.3 and later, the commands are:



cluster::*> network interface revert -vserver Cluster -lif
node1_clus2 and
cluster::*> network interface revert -vserver Cluster -lif
node2 clus2

34. Verify that all of the interfaces display true in the "Is Home" column: network interface show -vserver Cluster

The following example shows that all of the LIFs are up on node1 and node2 and that the "Is Home" column results are true:

cluster::*>	network int	erface show	-vserver Cluster		
	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2					
	clus1	up/up	10.10.11.1/16	node2	e1a
true					
	clus2	up/up	10.10.11.2/16	node2	e2a
true					

- 35. Ping the cluster ports to verify the cluster connectivity: cluster ping-cluster local

 The command output shows connectivity between all of the cluster ports.
- 36. Verify that both nodes have two connections to each switch: show isdp neighbors

 The following example shows the appropriate results for both switches:

Capability Code	es: R - Router, T S - Switch, H		_		age
Device ID Port ID	Intf	Holdtir	me Capabilit	y Platform	
					_
node1	0/1	132	Н	FAS3270	e1
node2	0/2	163	Н	FAS3270	e1
cs2	0/13	11	S	CN1610	
0/13					
cs2	0/14	11	S	CN1610	
0/14					
cs2	0/15	11	S	CN1610	
0/15					
cs2	0/16	11	S	CN1610	
0 /1 <i>c</i>					
	dp neighbors				
(cs2)# show isd	dp neighbors es: R - Router, T S - Switch, H				_dge
(cs2)# show isc Capability Code	es: R - Router, T	- Host, I	- IGMP, r - R		.dge
(cs2)# show iso Capability Code Device ID	es: R - Router, T S - Switch, H	- Host, I	- IGMP, r - R	Repeater	_dge
(cs2)# show iso Capability Code Device ID Port ID	es: R - Router, T S - Switch, H	- Host, I	- IGMP, r - R	Repeater	_dge -
(cs2)# show iso	es: R - Router, T S - Switch, H	- Host, I	- IGMP, r - R	Repeater	-
(cs2)# show isd Capability Code Device ID Port ID node1	es: R - Router, T S - Switch, H Intf	- Host, I - Holdtin	- IGMP, r - R me Capabilit	Repeater Ly Platform	- e2
(cs2)# show isd Capability Code Device ID Port ID node1 node2	es: R - Router, T S - Switch, H Intf	- Host, I - Holdtin	- IGMP, r - F me Capabilit 	Repeater Ty Platform FAS3270	- e2
(cs2)# show isd Capability Code Device ID Port ID node1 node2 cs1	es: R - Router, T S - Switch, H Intf 0/1 0/2	- Host, I - Holdtin	- IGMP, r - R me Capabilit H H	Repeater Ly Platform FAS3270 FAS3270	- e2
(cs2)# show isc Capability Code Device ID Port ID node1 node2 cs1 0/13	es: R - Router, T S - Switch, H Intf 0/1 0/2	- Host, I - Holdtin	- IGMP, r - R me Capabilit H H	Repeater Ly Platform FAS3270 FAS3270	- e2
(cs2) # show iscontinuous contents of the cont	es: R - Router, T S - Switch, H Intf 0/1 0/2 0/13	- Host, I - Holdtin	- IGMP, r - R me Capabilit H H S	Repeater Ly Platform FAS3270 FAS3270 CN1610	- e2
(cs2) # show iso Capability Code Device ID Port ID node1 node2 cs1 0/13 cs1 0/14	es: R - Router, T S - Switch, H Intf 0/1 0/2 0/13	- Host, I - Holdtin	- IGMP, r - R me Capabilit H H S	Repeater Ly Platform FAS3270 FAS3270 CN1610	- e2
(cs2) # show iscontinuous Capability Code Device ID Port ID node1 node2 cs1 0/13 cs1 0/14 cs1	es: R - Router, T S - Switch, H Intf 0/1 0/2 0/13 0/14	- Host, I - Holdtin Ho	- IGMP, r - R me Capabilit H H S S	Repeater Ly Platform FAS3270 FAS3270 CN1610 CN1610	- e2
0/16 (cs2) # show isc Capability Code Device ID Port ID node1 node2 cs1 0/13 cs1 0/14 cs1 0/15 cs1	es: R - Router, T S - Switch, H Intf 0/1 0/2 0/13 0/14	- Host, I - Holdtin Ho	- IGMP, r - R me Capabilit H H S S	Repeater Ly Platform FAS3270 FAS3270 CN1610 CN1610	-dge - e2 e2

- 37. Display information about the devices in your configuration: network device discovery show
- 38. Disable the two-node switchless configuration settings on both nodes using the advanced privilege command: network options detect-switchless modify

The following example shows how to disable the switchless configuration settings:

cluster::*> network options detect-switchless modify -enabled false



For release 9.2 and later, skip this step since the configuration is automatically converted.

39. Verify that the settings are disabled: network options detect-switchless-cluster show

The false output in the following example shows that the configuration settings are disabled:

```
cluster::*> network options detect-switchless-cluster show
Enable Switchless Cluster Detection: false
```



For release 9.2 and later, wait until Enable Switchless Cluster is set to false. This can take up to three minutes.

40. Configure clusters clus1 and clus2 to auto revert on each node and confirm:

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert true
```



For release 8.3 and later, use the following command: network interface modify -vserver Cluster -lif * -auto-revert true to enable auto-revert on all nodes in the cluster.

41. Verify the status of the node members in the cluster: cluster show

The following example shows information about the health and eligibility of the nodes in the cluster:

42. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

```
cluster::*> system node autosupport invoke -node * -type all -message
MAINT=END
```

43. Change the privilege level back to admin: set -privilege admin

Related information

Hardware Universe

NetApp CN1601 and CN1610 description page

CN1601 and CN1610 Switch Setup and Configuration Guide

NetApp KB Article 1010449: How to suppress automatic case creation during scheduled maintenance windows

Migrate to a two-node switched cluster in FAS22xx systems with a single cluster-network connection

If you have FAS22xx systems in an existing two-node switchless cluster in which each controller module has a single, back-to-back 10 GbE connection for cluster connectivity, you can use the switchless cluster networking option and replace the direct back-to-back connectivity with switch connections.

Before you begin

- Two cluster connections are required to migrate from a switchless configuration to a switched configuration.
- The cluster must be healthy and consist of two nodes connected with back-to-back connectivity.
- The nodes must be running ONTAP 8.2 or later.
- The switchless cluster feature cannot be used with more than two nodes.
- All cluster ports must be in the up state.

About this task

This procedure is a nondisruptive procedure that removes the direct cluster connectivity in a switchless environment and replaces each connection to the switch with a connection to the partner node.

Steps

 Change the privilege level to advanced, entering y when prompted to continue: set -privilege advanced

The advanced prompt (*>) appears.

2. Check the cluster status of the nodes at the system console of either node: cluster show

The following example displays information about the health and eligibility of the nodes in the cluster:

 $\hbox{3. Check the status of the HA pair at the system console of either node: $\verb|storage| failover| show } \\$

The following example shows the status of node1 and node2:

```
Node Partner Possible State Description

------
node1 node2 true Connected to node2
node2 node1 true Connected to node1

2 entries were displayed.
```

- 4. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: system node autosupport invoke -node * -type all -message MAINT=xh
 - x is the duration of the maintenance window in hours.



The message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster::*> system node autosupport invoke -node * -type all -message
MAINT=2h
```

- 5. Verify that the current state of the switchless cluster is true, and then disable the switchless cluster mode: network options switchless-cluster modify -enabled false
- 6. Take over the target node: storage failover takeover -ofnode target_node_name

It does not matter which node is the target node. When it is taken over, the target node automatically reboots and displays the Waiting for giveback... message.

The active node is now serving data for the partner (target) node that was taken over.

- 7. Wait for two minutes after takeover of the impaired node to confirm that the takeover was completed successfully.
- 8. With the target node showing the Waiting for giveback... message, shut it down.

The method you use to shut down the node depends on whether you use remote management through the node Service Processor (SP).

If SP	Then
Is configured	Log in to the impaired node SP, and then power off the system: system power off
Is not configured	At the impaired node prompt, press Ctrl-C, and then respond γ to halt the node.

- 9. On each controller module, disconnect the cable that connects the 10 GbE cluster port to the switchless cluster.
- 10. Connect the 10 GbE cluster port to the switch on both controller modules.
- 11. Verify that the 10 GbE cluster ports connected on the switch are configured to be part of the same VLAN.

If you plan to connect the cluster ports on each controller module to different switches, then you must verify that the ports on which the cluster ports are connected on each switch are configured for the same VLAN and that trunking is properly configured on both switches.

- 12. Give back storage to the target node: storage failover giveback -ofnode node2
- 13. Monitor the progress of the giveback operation: storage failover show-giveback
- 14. After the giveback operation is complete, confirm that the HA pair is healthy and takeover is possible: storage failover show

The output should be similar to the following:

Node	Partner	Possible	State Description
node1 node2	node2 node1	true true	Connected to node2 Connected to node1
2 entries were displayed.			

15. Verify that the cluster port LIFs are operating correctly: network interface show -role cluster

The following example shows that the LIFs are up on node1 and node2 and that the "Is Home" column results are true:

```
cluster::*> network interface show -role cluster
          Logical Status Network
                                            Current
Current Is
Vserver Interface Admin/Oper Address/Mask
                                            Node
                                                        Port
Home
node1
        clus1 up/up 192.168.177.121/24 node1
                                                        e1a
true
node2
         clus1 up/up 192.168.177.123/24 node2
                                                        e1a
true
2 entries were displayed.
```

16. Check the cluster status of the nodes at the system console of either node: cluster show

The following example displays information about the health and eligibility of the nodes in the cluster:

- 17. Ping the cluster ports to verify the cluster connectivity: cluster ping-cluster local

 The command output should show connectivity between all of the cluster ports.
- 18. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

```
cluster::*> system node autosupport invoke -node * -type all -message
MAINT=END
```

19. Change the privilege level back to admin: set -privilege admin

Related information

NetApp KB Article 1010449: How to suppress automatic case creation during scheduled maintenance windows

CN1601 and CN1610 Switch Setup and Configuration

Details how to configure the switch hardware and software for your cluster environment.

Setup and Configuration

CN1610 Network Switch CLI Command Reference - Version 1.2.x.x

Details of the command-line interface (CLI) commands you use to configure the CN1610 software.

Command Reference

CN1610 Network Switch CLI Command Reference - Version 1.2.x.x

Details of the command-line interface (CLI) commands you use to configure the CN1610 software.

Command Reference

NetApp 10G Cluster-Mode Switch Installation

An overview of the CN1610 switch hardware and software features and describes the features to install the switch and access the CLI.

10G Installation Guide

NetApp CN1610 Switch Administrator's Guide - Version 1.1.x.x

Examples of how to use the CN1610 switch in a typical network.

Administrator's Guide

NetApp CN1610 Switch Administrator's Guide - Version 1.2.x.x

Examples of how to use the CN1610 switch in a typical network.

Administrator's Guide

CN1601 Network Switch CLI Command Reference

Details of the command-line interface (CLI) commands you use to configure the CN1601

software.

Command Reference

CN1601 Switch Administrator

Examples of how to use the CN1601 switch in a typical network.

Administrator's Guide

NetApp 1G Cluster-Mode Switch Installation

An overview of the CN1601 switch hardware and software features and installation process.

1G Installation Guide

NVIDIA MSN2100 Switches

Other switch models

Other Cisco Cluster, Storage and Management Switches

You can use the link below to access documentation for the following switches:

- Cisco Nexus 5596
- NetApp CN1601

Documentation for other Cisco Cluster, Storage and Management Switches

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for disk shelves

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

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

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.